

Descriptive analysis of wide area network flow control internet traffic on Metro-E 100 Mbps campus network

Nor Paezah Abdullah^{1,4}, Murizah Kassim^{1,2}, Sayang Mohd Deni³, Yusnani Mohd Yusoff¹

¹School of Electrical Engineering, College of Engineering, Universiti Teknologi MARA, Selangor, Malaysia

²Institute for Big Data Analytics and Artificial Intelligence (IBDAAI), Universiti Teknologi MARA, Selangor, Malaysia

³College of Computing, Informatics, and Media Studies, Universiti Teknologi MARA, Selangor, Malaysia

⁴Institut Kemahiran Tinggi PERDA (PERDA-TECH), Pulau Pinang, Malaysia

Article Info

Article history:

Received Jun 21, 2023

Revised Feb 26, 2024

Accepted Mar 6, 2024

Keywords:

Campus network

Descriptive analysis

Internet traffic flow

Quality of service

Wide area network Metro-E

ABSTRACT

QoS in computer networking is the capability to provide better service to network traffic over various technologies such as ethernet and IP networks. This paper presents a descriptive analysis of WAN flow control and internet traffic on a Metro-E campus network. Issues on network congestion and delay in network QoS where internet traffic is gradually increasing, resulting in bursts of network capacity that affect network QoS. The method implies 12 months data collection and analysis on protocol, bytes and packets inbound and correlation between parameters on the Metro-E 100 Mbps campus network. The result presents heavy-tailed distributions on an inbound packet kurtosis value of 347 and an outbound packet kurtosis value of 780. Bytes outbound and inbound are skewed at 122 and right at 17 respectively. The average amount of data inbound and outbound is 458.5 MB and 34.8 MB. Protocol 6 TCP presents the highest amount of traffic and a weak positive correlation at 0.104 exists between the inbound and outbound packets and bytes on the network. The correlation coefficient's 95% confidence interval ranges between 0.096 and 0.111. This research is significant in the future deployment of traffic scheduling, policing, and shaping algorithms for QoS bandwidth management on the WAN Metro-E campus network.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Murizah Kassim

Institute for Big Data Analytics and Artificial Intelligence (IBDAAI), Universiti Teknologi MARA

40450 Shah Alam, Selangor, Malaysia

Email: murizah@uitm.edu.my

1. INTRODUCTION

The rapid advancement of broadband, especially fiber-optic technology, and 5G, has increased internet usage among home and campus network users, particularly for multimedia applications with high bandwidth requirements, like online meetings, online classes, and streaming applications. The increased capacity provided by simultaneous deployment of different radio and fixed access networks for Wi-Fi, long-term evolution (LTE), 5G, and digital subscriber line (DSL) offers the potential for improved service offering to home, campus, and business users particularly for bandwidth-hungry live and streaming multimedia applications [1]. On-demand videos, long-term evolution, and VoIP are some of the packet-based applications that are growing fast. So, it is necessary to upgrade the current network connections to manage traffic and improve the network's quality of service (QoS) [2]. A wide area network (WAN) can be developed over a metropolitan area using metro ethernet technology. It enables high-speed, secure communication between remote office locations, offering enterprise-level functionality and quicker speeds

than those provided by more conventional technologies like T1/T3 [3]. Network protocols can be thought of as languages that two devices, regardless of the differences in their infrastructure and designs, must be able to communicate with one another. Three types of network protocol are used at the WAN Metro-E 100 Mbps campus network which are protocol 1, internet control message protocol (ICMP), protocol 6, transmission control protocol (TCP), and protocol 17, user datagram protocol (UDP). Out-of-band messages relating to network operation or malfunction are sent via ICMP messages that are sent in IP packets [4]. Through flow control and data acknowledgment, TCP delivers comprehensive error checking. Data packets must arrive at the receiving end in the correct order, and TCP guarantees this [5]. While, UDP does not have any dependability, flow control, or error recovery features compared to TCP and when the TCP dependability mechanisms are not required, UDP is helpful [6].

The effective utilization of bandwidth, path loss rate, and latency can be measured to optimize network performance [7], [8]. It is expensive to maintain optimal WAN bandwidth, and failure can cause congestion-related packet loss. Streaming media like YouTube, Netflix, and Facebook among others put a strain on the campus network's bandwidth [9]. Therefore, an analysis of traffic characteristics through network protocol and QoS performance is needed to ensure bandwidth allocation for a campus network. The usage of network resources needs to be monitored to avoid network congestion. Packet loss rate, queue delay, network throughput, and network resource utilization like queues are important parameters for network performance optimization [10]. WAN Metro-E campus network uses high bandwidth to satisfy the user needs, and numerous internet-based applications, including video streaming, cloud computing, and online streaming services [11]. The QoS in network management such as bandwidth, processing time, and performance often experience traffic bursts in the network although, the network speed is upgraded from time to time to accommodate the increase of internet application services [12]. Reliable QoS of network traffic can be achieved with the help of proper network control and monitoring techniques to improve connections [13]. The analysis must be carried out on the real-time network traffic, to understand the situation of internet traffic [14].

Two problems that impact the operation of a WAN are congestion and flow control. Congestion occurs when the demand for network resources exceeds the available capacity, resulting in decreased performance and possibly packet loss. High levels of congestion can cause higher delay, packet loss, reduced throughput, and poor QoS for end users [15]. Congestion can be caused by several circumstances, including high network traffic, network equipment failures, inefficient routing methods, and network misconfigurations [16]. Meanwhile, flow control systems govern the velocity of data transfer across network devices to avoid overwhelming the receiving end and ensure stable connection. Flow control techniques can prevent network congestion by controlling the quantity of data transmitted at any time which impacts the network performance [17]. Without proper flow management, data packets may be lost or dropped due to buffer overflows or processing delays, resulting in retransmissions and poor performance. Flow control problems can occur owing to mismatches in data transfer speeds between sender and recipient, network congestion, or incompatible protocols [18].

Increasing the network's bandwidth capacity is another technique to overcome network congestion such as artificial intelligence [19]. This can be accomplished by expanding the network or by updating the network's infrastructure [20], [21]. Other strategies by using QoS protocols to prioritize certain types of traffic such as policing and shaping internet traffic [22]. This can ensure that important traffic like audio and video traffic, which is more crucial, receives precedence over less crucial traffic like file downloads. Congestion and flow control problems can also be discovered early on with regular network monitoring. Network monitoring and flow control typically involve specialized network monitoring software and R is a powerful statistical analysis tool. Monitoring network traffic serves as a safety network and early warning system for potential issues, as well as a means of maintaining network performance and speed [23]. Network traffic analysis is the process of recording, reviewing, and analyzing network traffic for performance, security, and/or network operations and general management [24]. It is a process of using manual and automated techniques to check details and detail-level statistics in network traffic [25]. Traffic engineering, quality of service, and anomaly detection also depend on monitoring for decision-making [26]. Network traffic analysis and predictions have become vital for monitoring networks, while network prediction is the process of capturing network traffic and examining it deeply to decide what is the occurrence in the network [27]. Traffic classification of the network is an important requirement to optimize traffic engineering and adequately provision QoS [28]. Campus networks offer a rich and fertile environment to study current trends in network application usage because high-speed network connectivity keeps growing from time to time [29].

This paper presents a descriptive analysis of WAN flow control internet traffic on the Metro-E 100 Mbps campus network. Enhancing the bandwidth management on the metro-E network is the study's aim and outcome measure. Descriptive analysis is used as a guide and a point of reference to manage internet-protocol bandwidth management on the Metro-E campus or other networks to provide the best QoS for managing internet traffic. Data was collected for 12 months starting from 21st August 2021 until 21st August 2022 on the campus network using Exinda Network Orchestrator. Packet, bytes, and throughput

internet traffic were analyzed based on six main areas which are the protocol, inbound and outbound packet, inbound and outbound bytes, correlation on packets inbound against outbound, correlation on bytes inbound against outbound, and packet inbound against outbound interval. The significance of the analysis is that the results will be used in future research endeavors. This study has the potential to change how WAN Metro-E campus networks are managed and optimized in real-world situations. Improved traffic scheduling and bandwidth management can result in higher network dependability, performance, and resource usage. The analyzed data will be fitted to a statistical model to better understand the underlying patterns or correlations. The analysis results will be used to optimize network performance and effectively manage bandwidth, as well as to deploy algorithms to improve QoS bandwidth management.

2. METHOD

The methodology and resources utilized for the analysis are described in this section. The desired outcomes are thoroughly explained in the flowchart and activities. The methodology consists of data collection using Exinda tools and traffic data of characterizations can be analyzed and plotted into graphs. The analysis must be carried out on the real-time network traffic, to understand the situation of campus network traffic.

2.1. Research framework

A research framework has been planned that takes action to analyze the WAN control flow and traffic performance. Figure 1 presents the research framework that shows the steps from data collection, data analysis, descriptive analysis, and documentation.

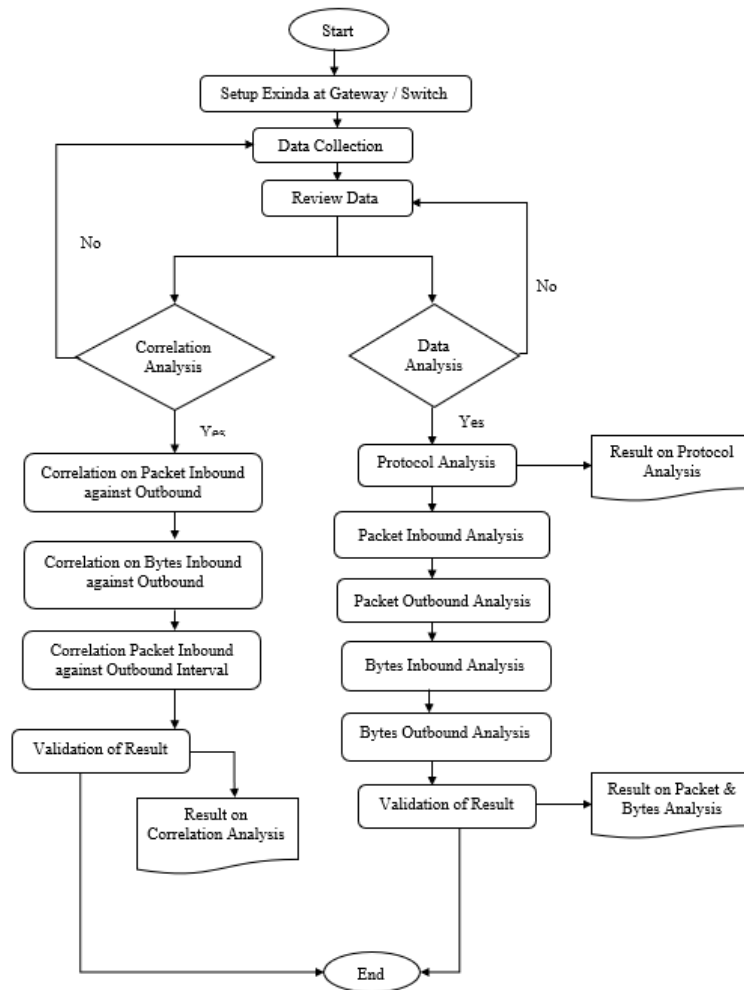


Figure 1. Research framework

Exinda Network Orchestrator will be installed on a Gateway Switch as a network monitoring device for data gathering. Data on WAN internet traffic will be gathered every 10 seconds between arrival times and compiled into 1 hour each month at 100 Mbps Metro-E campus networks. Data on internet traffic was gathered for a full year, from August 1, 2021, to August 31, 2022. A descriptive statistical analysis method utilizing the R language and Pareto distribution will be utilized to describe the flow control of internet traffic. Protocol analysis, packet inbound, and outbound analysis, bytes inbound and outbound analysis, as well as packet and bytes inbound outbound parameter analysis were all included in the comparison analysis of the relationship on packet inbound against outbound, bytes inbound against outbound, and packet inbound against outbound interval.

2.2. Exinda monitoring tools

The Exinda Network Orchestrator, on the other hand, was created to gather data for additional analysis and/or to analyze the performance of certain applications. Exinda Network Orchestrator is a simple-to-use tool that enables users to monitor network traffic, provide the necessary level of performance for mission-critical IT services, and quickly identify and fix network issues. Exinda is a utility that controls network monitoring as well as provides bandwidth control for linked computer devices [30]. Using the Exinda appliance to achieve network optimization, users may observe and assess their performance in the network and the application. Certain monitoring solutions, like the Exinda SD-WAN, can provide network monitoring with real-time management data [31].

2.3. Data collection and descriptive analysis

Data on packets, bytes, and throughput on the WAN Metro-E 100 Mbps campus network were collected from August 1st, 2021, until August 31, 2022, using the Exinda Network Orchestrator. The analysis will describe the relationship between throughput inbound and outbound as well as the shape of the data. Furthermore, by using the information on the shape of the data, the peak usage periods must be seen clearly. Descriptive analysis of WAN flow control for internet traffic on a Metro-E campus network involves examining the characteristics and patterns of the network traffic. Using R, exploratory analysis using a mean, and median function to obtain summary statistics of relevant variables, such as packet counts, data rates, or latency and can visualize traffic patterns and visualize the distribution of variables by using histogram plots to examine the distribution of packet counts or data rates. The time-series plot uses line plots to visualize how traffic varies over time. This can help identify peak usage periods or recurring patterns. Meanwhile, correlation analysis identifies relationships by computing correlation coefficients using functions to examine relationships between variables, such as packet counts, latency, and data rates by using R [32].

3. RESULTS AND DISCUSSION

The results of the descriptive analysis of WAN flow control internet traffic on the Metro-E 100 Mbps campus network is crucial in the process of developing optimal network performance. The outcome will be a manual for figuring out the characteristics of internet traffic based on the internet protocol network for bandwidth control and QoS Internet promising to satisfy the requirements of the Metro-E campus network. The outcomes of the study of the twelve months of data will be used to assess the design of a network system that is more successful at managing bandwidth to satisfy user needs.

3.1. Protocol analysis

Studying the structure, syntax, and semantics of the network communication protocols is necessary to identify potential vulnerabilities and performance issues. WAN Metro-E campus network used 3 types of protocol in the network, protocol 1 (ICMP), protocol 6 (TCP), and protocol 17 (UDP). Based on Table 1 for inbound bytes, protocol 1, has a mean value of 8863 Mbps, a median value is 0, and a standard deviation of 53402 Mbps. The data is positively Right-Skewed with a skewness value of 8.32 and has a high kurtosis at 79.15 that shows a high peak on the distribution. Protocol 6, there is a mean value of 336792 Mbps, a median value is 20452 Mbps, and a standard deviation of 1909165 Mbps. The data is highly positively right skewed with a skewness value of 16.01 and has a very high kurtosis at 326.17 showing a very high peak in the distribution. Meanwhile, for protocol 17, there is a mean value of 381849 Mbps, a median value is 81990 Mbps, and a standard deviation of 1642769 Mbps. The data is also highly positively skewed with a skewness value of 17.01 and has a very high peak on distribution with a kurtosis value of 454.42. In terms of central tendency, protocol 17 looks to have the highest mean and a relatively high median, implying that it may perform better in handling inbound packets than the other protocols. The high skewness and kurtosis in all three protocols, on the other hand, suggest that the distributions are not normal and have heavy tails, which could be related to outliers or special data peculiarities.

Table 1. Network protocol on inbound and outbound bytes

	Protocol	Mean (Mbps)	Median (Mbps)	Standard deviation (Mbps)	Skewness	Kurtosis
Inbound bytes	1	8863	0	53402	8.32	79.15
	6	336792	20452	1909165	16.01	326.17
	17	381849	81990	1642769	17.01	454.42
Outbound bytes	1	9143	10	53812	8.34	79.68
	6	214952	20657	1335717	21.32	702.04
	17	154504	33098	725377	20.51	662.16

However, for the packet's outbound variable, protocol 1 (ICMP) with a mean value of 9,143 Mbps shows traffic has a comparatively low data rate, indicating a low degree of activity. The presence of outliers or various traffic patterns suggests that the standard deviation is 53,812 Mbps, indicating high diversity in data rates. The positive skewness score of 8.34 indicates that higher values are dragging the distribution to the right, possibly because of infrequent high data rate events. Meanwhile, kurtosis on 79.68 indicates large tails and probable outliers, implying that there may be instances of exceptionally high or low data rates. Besides that, protocol 6 (TCP) with a mean value of 214,952 Mbps exhibits a high mean data rate, indicative of substantial data transmission associated with TCP. Standard deviation value of 1,335,717 Mbps suggests significant variability in TCP data rates, potentially driven by extreme outliers. Meanwhile, the extremely positive skewness of 21.32 highlights the bursty nature of TCP traffic, and the exceptionally high kurtosis indicates heavy tails and a distribution prone to extreme values, emphasizing the presence of outliers. protocol 17 (UDP) with a mean value of 54,504 Mbps shows moderate data transmission. The high standard deviation with a value of 725,377 Mbps indicates considerable variability in data rates, potentially influenced by outliers or diverse traffic patterns. Meanwhile, extremely positive skewness suggests a concentration of lower data rates with the potential for sporadic high data rate occurrences. A very high kurtosis 662.16 value implies heavy tails and potential outliers, indicating that data rates can exhibit extreme values.

Protocol 6 shows significant data transmission with a bursty nature and potential outliers, while protocol 1 shows minimal activity with a broad range of data rates, and protocol 17 shows moderate data transmission with variability and the potential for extreme values. Figure 2 shows the 6 protocol analysis generated the most inbound and outbound traffic on the network.

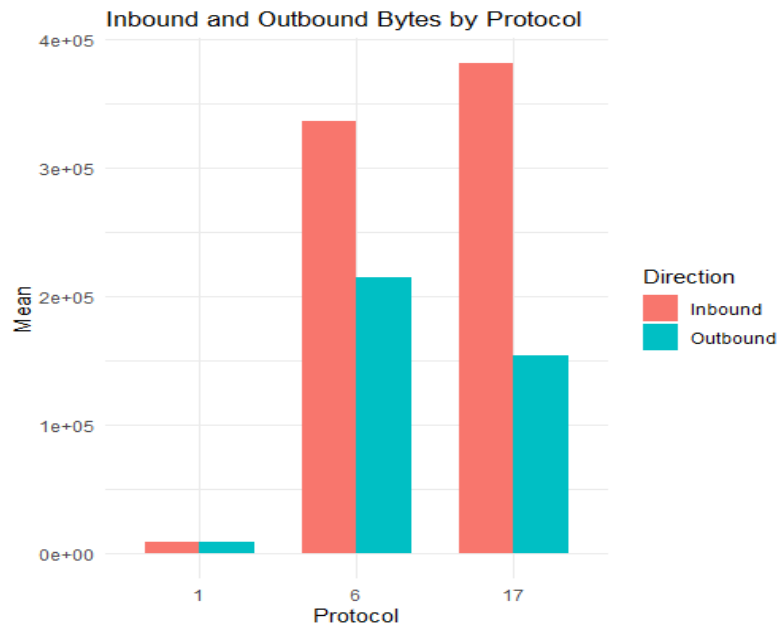


Figure 2. Protocol analysis

3.2. Analysis of inbound and outbound packets

An essential part of network security and monitoring is packet analysis, which can assist in guaranteeing that networks are dependable, secure, and function well across many locations. In order to

identify potential problems like security vulnerabilities, network performance concerns, and other network-related issues, inbound and outbound packet analysis comprises looking at the traffic traveling between different nodes and devices on the network. Table 2 shows the inbound packets have a higher mean of 344,902 MB compared to outbound packets of 202,229 MB, showing the average number of packets inbound that are received more than the sent outbound packets. Meanwhile, inbound packets have a higher median of 37,977 MB compared to outbound packets of 24,320 MB. Both inbound and outbound packets have high standard deviations 1,856,115 MB for inbound and 1,235,812 MB for outbound.

Table 2. Inbound and outbound packet

Packets	Mean (MB)	Median (MB)	Standard deviation (MB)	Skewness	Kurtosis	Maximum (MB)
Inbound	344,902	37,977	1,856,115	16.24	347	75,261,807
Outbound	202,229	24,320	1,235,812	22.30	780	79,085,741

This indicates significant variations in packet counts, potentially indicating fluctuations in network traffic. Inbound packets have a positive skewness value at 16.24 indicating a highly skewed distribution with a long tail to the right. Outbound packets have an even higher positive skewness value of 22.30, suggesting an even more skewed distribution. The high skewness values indicate that most packets are concentrated towards the lower end of the distribution, with a few extremely high values on the right tail. Inbound packets have a kurtosis value of 347, while outbound packets have a kurtosis value of 780. Both values indicate heavy-tailed distributions. The high kurtosis values suggest that there are significant outliers or extreme values in the packet count distribution, indicating potential bursts or anomalies in network traffic. The maximum size of an inbound packet is 75,261,807 MB, whereas the outbound packet is 79,085,741 MB. Understanding the upper bounds of packet counts and spotting any instances of unusually high traffic can both benefit from knowing these maximum values. Figure 3 shows that the packet distributions are highly variable, skewed, and heavy-tailed. Network delays and possible congestion are indicated by the large fluctuation in packet counts and the presence of skewed distributions. To preserve good network operation, they require appropriate traffic management solutions.

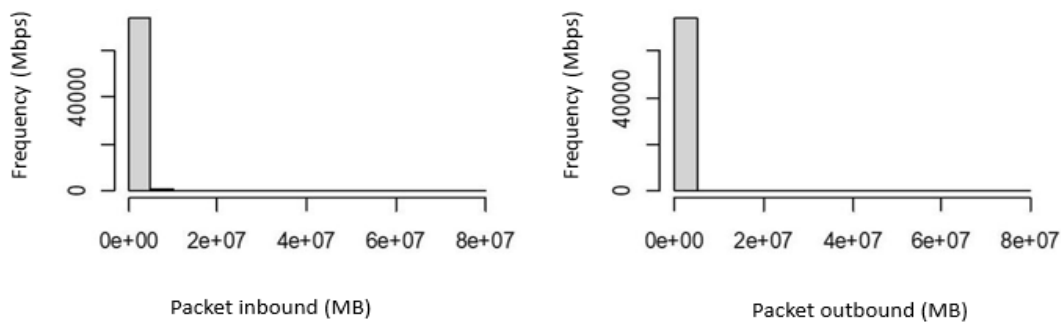


Figure 3. Packet inbound and outbound analysis

3.3. Analysis of inbound and outbound bytes

Analyzing inbound and outbound bytes involves monitoring and measuring the volume of data transmitted and received across the network. The information can help to identify network traffic patterns, assess bandwidth utilization, and troubleshoot performance issues. Table 3 shows the mean value of inbound bytes 458.5 MB is much higher than the outbound bytes 34.8 MB. On average, more bytes are received by the network compared with sent-out bytes. However, the range of values for bytes inbound is much larger than outbound, as indicated by the maximum values of mean and median.

Table 3. Inbound and outbound bytes

Bytes	Mean (MB)	Median (MB)	Standard deviation (MB)	Skewness	Kurtosis	Maximum (MB)
Inbound	458.5	17.6	2,600.4	17	363	108,000
Outbound	34.8	3.2	707.8	122	17,873	112,000

The mean and median values for both inbound and outbound data are significantly different, indicating the presence of outliers or skewness, and compared to outbound data, inbound data has a much larger mean and median, indicating a rightward skewness. The standard deviation for inbound data is 2600.4 MB, indicating a bigger spread or variability in the data points. Kurtosis values suggest that the distribution is heavy-tailed, especially for outbound data. The highest value especially for outbound data 112,000 MB, implying that outliers or extreme values exist in both datasets. The nature of extreme values suggests that they may indicate peak usage or potential issues.

Figure 4 shows the distribution of bytes inbound, 17 is heavily skewed to the right, with a long tail of extreme values. On the other hand, bytes outbound are highly skewed, 122 to the right, this means that there are some very large inbound traffic spikes in the data, which might be indicative of certain events or activities on the network. Meanwhile, the highly skewed distribution indicates that certain events or activities are creating considerable outbound data flow, potentially affecting network resources.

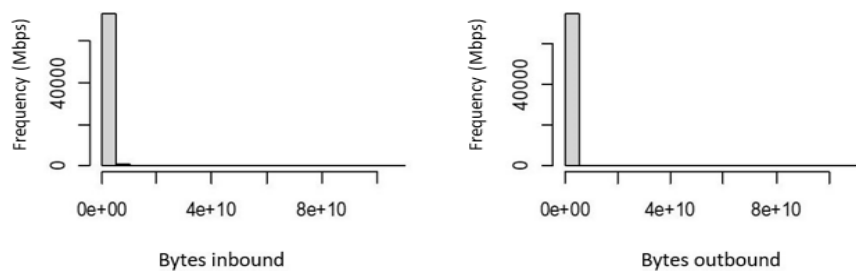


Figure 4. Inbound and outbound bytes

3.4. Correlation of packets inbound against outbound

A correlation between inbound and outbound packets can provide insights into network performance, traffic patterns, and potential issues within the local network. It's important to consider other factors that may influence the correlation, such as network architecture, traffic management policies, congestion, and network equipment capabilities. This analysis identifies potential network issues, bottlenecks, or asymmetries in traffic flow within the campus network. Figure 5 visualizes the relationship between the variables, and it shows the resulting value of the correlation coefficient is 0.938, which suggests a strong positive correlation between packet inbound against outbound. The resulting p-value is less than $2.2e-16$, which is less than the significance level of 0.05, indicating strong evidence against the null hypothesis. The confidence interval for the correlation coefficient is between 0.937 and 0.938, which suggests a very strong positive correlation between the two variables.

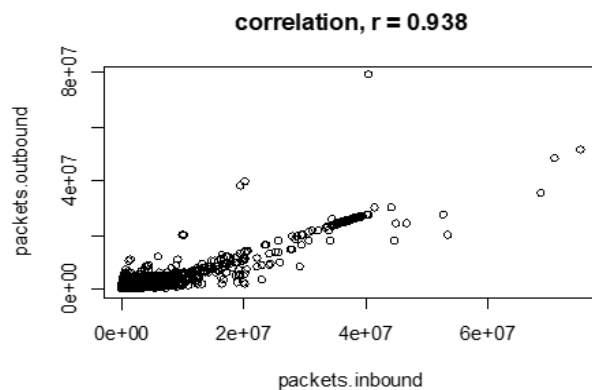


Figure 5. Correlation of packets inbound against outbound

The correlation is close to 1 suggesting that as inbound packets increase, outbound packets also tend to increase proportionally. Overall, strong statistical evidence supports a positive correlation between inbound and outbound packets in the WAN Metro-E campus network, indicating that the two variables are

highly related. Three different correlations of packets inbound against packets outbound for protocol 1, protocol 6, and protocol 17 was presented. A positive relationship between packets inbound and outbound where protocols 6 and 17 showed a high positive correlation, whereas the relationship for protocol 1 was a moderate positive correlation. Optimization efforts can be focused on maintaining a balance between inbound and outbound traffic to prevent bottlenecks or performance issues. Figure 6 shows the relationship for protocol 1 is moderately positive correlation with a value of 0.527. A moderately positive correlation of 0.527 suggests that as the number of inbound packets associated with protocol 1 increases, the number of outbound packets also tends to increase, but the relationship is not exceptionally strong.

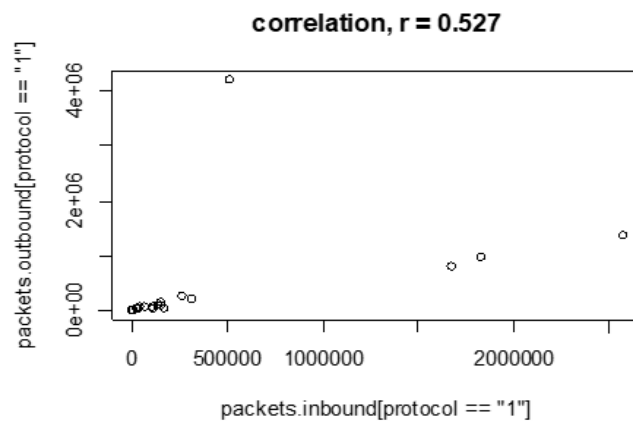


Figure 6. Correlation of packets inbound against outbound for protocol 1

Figure 7 shows a strength of the correlation for protocol 6 with $r=0.944$ falls in the very strong range. A strong positive correlation, suggesting an even more robust relationship as the number of inbound packets associated with protocol 6 increases, the number of outbound packets also tends to increase. The relationship indicates an efficient and well-balanced network or system in handling the traffic associated with protocol 6.

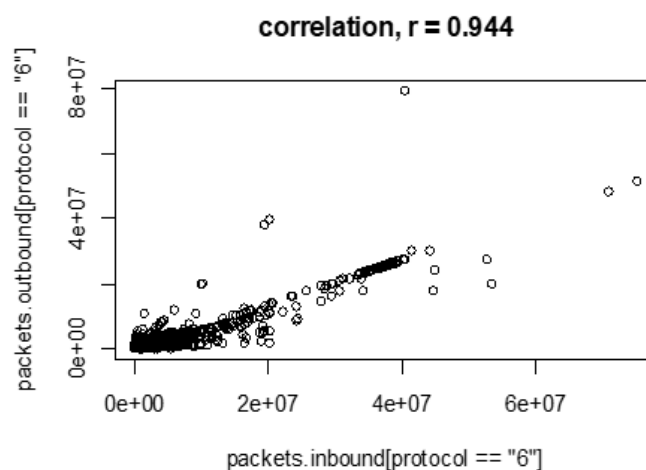


Figure 7. Correlation of packets inbound against outbound for protocol 6

Figure 8 presents the correlation between packets inbounds against outbound for protocol 17 shows a positive relationship with a value of 0.912. A correlation coefficient of 0.912 is very close to 1, indicating an extremely strong positive correlation, suggesting a robust relationship as the number of inbound packets associated with protocol 17 increases, the number of outbound packets also increases, and the relationship is notably strong.

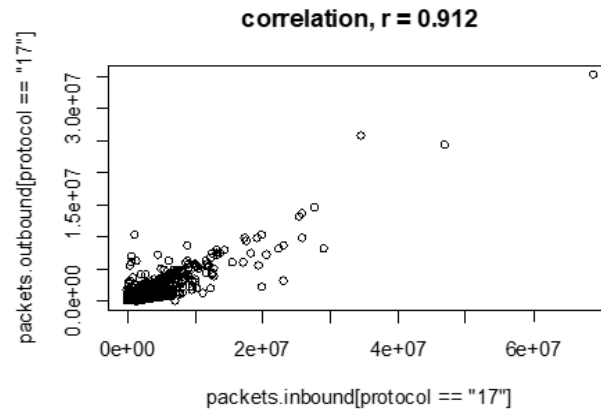


Figure 8. Correlation of packets inbound against outbound for protocol 17

3.5. Correlation of bytes inbound against outbound

Correlation analysis is a statistical method that assesses linear relationships. It may not capture more complex relationships or dependencies in the network data. Other factors, such as network topology, traffic patterns, or specific application behaviors, may influence the relationship between inbound and outbound bytes on the WAN Metro-E campus network. Figure 9 illustrates the correlation coefficient between bytes inbounds and outbound. There is a positive correlation between the two variables, indicating that as inbound traffic increases outbound traffic also tends to increase. However, there are some outliers or extreme values in the data, as indicated by the points in the upper right corner of the plot. The resulting value of the correlation coefficient is 0.104, which suggests a weak positive correlation between the two variables. The p-value obtained from the correlation test indicates that this correlation is statistically significant at a significant level of 0.05. The weak positive correlation suggests a limited association between inbound and outbound bytes. While there is a tendency for them to increase together, the relationship is not strong. A weak correlation might indicate that changes in one direction of traffic do not necessarily require a proportional response in the other direction.

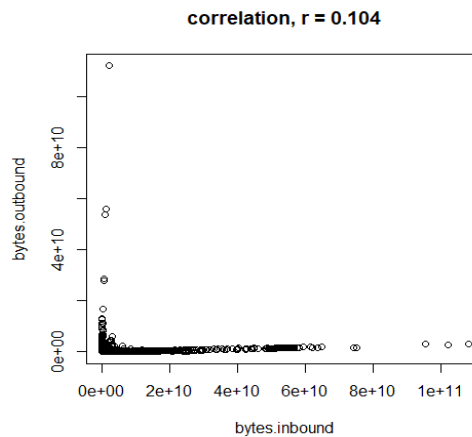


Figure 9. Correlation of bytes inbound against outbound

3.6. Correlation of packets Inbound against outbound interval

Analyzing the relationship between packet inbound and outbound intervals on a WAN Metro-E campus network, gain valuable insights into network performance, capacity planning, QoS management, network troubleshooting, traffic patterns, and security. Figure 10 shows the relationship between inbound and outbound intervals shows a strongly high positive correlation with $r=0.985$. The high correlation suggests that the network exhibits a high degree of efficiency and synchronization between inbound and outbound intervals. The relationship identifies the volume and distribution of inbound and outbound traffic, allowing

for assessment of the overall network utilization and identifying potential congestion points or bottlenecks and also assists in optimizing network traffic by helping to identify the types of traffic dominating the network, to prioritize critical applications or services, and allocate bandwidth accordingly. High volumes of inbound or outbound traffic can impact network performance. Excessive inbound traffic may lead to congestion and affect the response time of services, while high outbound traffic may strain the network's capacity to send data to external destinations.

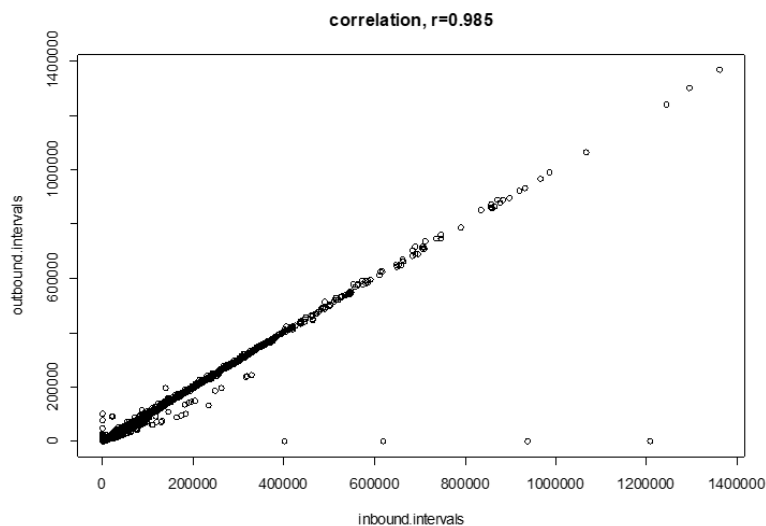


Figure 10. Packet inbound against outbound intervals

4. CONCLUSION

The analysis of WAN flow control and internet traffic on the Metro-E campus network, addressing network performance for congestion and delay issues of QoS on the internet WAN. The analysis provides valuable information into the network's characteristics and patterns that show protocol 6 which is TCP generates the highest amount of traffic. This information helps prioritize resource allocation and implement specific measures for managing the traffic generated by different protocols. The inbound and outbound packet analysis shows significant variations in packet counts, high standard deviations, and skewed distributions. These characteristics indicate the potential for congestion and network delays. Meanwhile, through packet analysis, the inbound and outbound bytes demonstrate substantial variability and skewed distributions. There is a strong positive correlation between inbound and outbound packets, suggesting a close relationship between these variables. The correlation of packet inbound and outbound intervals shows a balanced distribution of packet counts between incoming and outgoing network traffic. Traffic shaping or QoS policies can be implemented to ensure optimal network performance by understanding the inbound and outbound flow and a symmetrical flow of data within the network. In summary, the analysis underscores the importance of effective traffic management strategies to address congestion, optimize resource utilization, and enhance the overall performance of the WAN Metro-E campus network. Overall, this study contributes to a better understanding of WAN flow control and internet traffic in a Metro-E campus network, paving the way for improved network management and optimization. The results of this analysis will be used for future research in fitting the data with a statistical model and implementing the policing and shaping procedure for QoS bandwidth control on the Metro-E campus network.

ACKNOWLEDGEMENTS

Authors acknowledge the Universiti Teknologi MARA for funding under the Geran Insentif Penyelidikan no (600-RMC/GIP 5/3/ (087/2023).

REFERENCES




- [1] A. S. Sadeq, R. Hassan, S. S. Al-Rawi, A. M. Jubair, and A. H. M. Aman, "A Qos Approach For Internet Of Things (Iot) Environment Using Mqtt Protocol," in *2019 International Conference on Cybersecurity (ICoCSec)*, Sep. 2019, pp. 59–63, doi: 10.1109/ICoCSec47621.2019.8971097.

- [2] M. A. Ridwan, N. A. M. Radzi, W. S. H. M. Wan Ahmad, F. Abdullah, M. Z. Jamaludin, and M. N. Zakaria, "Recent trends in MPLS networks: technologies, applications and challenges," *IET Communications*, vol. 14, no. 2, pp. 177–185, Jan. 2020, doi: 10.1049/iet-com.2018.6129.
- [3] M. Rapisarda *et al.*, "All-optical aggregation and distribution of traffic in large metropolitan area networks using multi-Tb/s S-BVTs," *Journal of Optical Communications and Networking*, vol. 14, no. 5, pp. 316–326, May 2022, doi: 10.1364/JOCN.448115.
- [4] M. F. Abbood, M. F. Kadhim, and A. R. Kadhim, "Improving multimedia data transmission quality in wireless multimedia sensor networks through priority-based data collection," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 4, pp. 3595–3606, Aug. 2022, doi: 10.11591/ijece.v12i4.pp3595-3606.
- [5] H. K. Ravuri, M. T. Vega, J. Der Van Hooft, T. Wauters, and F. De Turck, "Adaptive Partially Reliable Delivery of Immersive Media Over QUIC-HTTP/3," *IEEE Access*, vol. 11, pp. 38094–38111, 2023, doi: 10.1109/ACCESS.2023.3268008.
- [6] V. K. Jain, A. P. Mazumdar, P. Faruki, and M. C. Govil, "Congestion control in Internet of Things: Classification, challenges, and future directions," *Sustainable Computing: Informatics and Systems*, vol. 35, p. 100678, Sep. 2022, doi: 10.1016/j.suscom.2022.100678.
- [7] A. Malik, M. Z. Khan, S. M. Qaisar, M. Faisal, and G. Mehmood, "An Efficient Approach for the Detection and Prevention of Gray-Hole Attacks in VANETs," *IEEE Access*, vol. 11, pp. 46691–46706, 2023, doi: 10.1109/ACCESS.2023.3274650.
- [8] U. Musa, S. Babani, S. A. Babale, A. S. Ali, Z. Yunusa, and S. H. Lawan, "Bandwidth enhancement of millimeter-wave microstrip patch antenna array for 5G mobile communication networks," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 4, pp. 2203–2211, Aug. 2023, doi: 10.11591/eei.v12i4.4680.
- [9] H. Bege and A. Y. Zubairu, "Campus realities: Forecasting user bandwidth utilization using monte carlo simulation," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 5, pp. 4809–4817, Oct. 2020, doi: 10.11591/ijece.v10i5.pp4809-4817.
- [10] Z. Tian, "Chaotic characteristic analysis of network traffic time series at different time scales," *Chaos, Solitons & Fractals*, vol. 130, p. 109412, Jan. 2020, doi: 10.1016/j.chaos.2019.109412.
- [11] R. B.-Mariscal, P. C. S.-Mancilla, O. A. M.-López, M. V.-Briseno, and J. I. N.-Hipolito, "Prioritization-Driven Congestion Control in Networks for the Internet of Medical Things: A Cross-Layer Proposal," *Sensors*, vol. 23, no. 2, p. 923, Jan. 2023, doi: 10.3390/s23020923.
- [12] A. A. Ghafar, M. Kassim, N. Ya'acub, R. Mohamad, and R. A. Rahman, "QoS of Wi-Fi performance based on signal strength and channel for indoor campus network," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 5, pp. 2097–2108, Oct. 2020, doi: 10.11591/eei.v9i5.2251.
- [13] N. P. Abdullah, S. M. Deni, and M. Kassim, "WAN Internet Traffic Parameter Analysis on Metro-E Campus Network," in *2023 IEEE 14th Control and System Graduate Research Colloquium (ICSGRC)*, Aug. 2023, pp. 180–185, doi: 10.1109/ICSGRC57744.2023.10215487.
- [14] N. P. Abdullah, M. Kassim, and Y. M. Yusoff, "Analysis of Internet Application Services Traffic on WAN Metro-E Network," in *2022 IEEE 13th Control and System Graduate Research Colloquium (ICSGRC)*, Jul. 2022, pp. 209–214, doi: 10.1109/ICSGRC55096.2022.9845156.
- [15] M. N. Khan *et al.*, "Energy-Efficient Dynamic and Adaptive State-Based Scheduling (EDASS) Scheme for Wireless Sensor Networks," *IEEE Sensors Journal*, vol. 22, no. 12, pp. 12386–12403, Jun. 2022, doi: 10.1109/JSEN.2022.3174050.
- [16] X. Zhong, J. Zhang, Y. Zhang, Z. Guan, and Z. Wan, "PACC: Proactive and Accurate Congestion Feedback for RDMA Congestion Control," in *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*, May 2022, pp. 2228–2237, doi: 10.1109/INFOCOM48880.2022.9796803.
- [17] H. Xie and T. Li, "Revisiting Loss Recovery for High-Speed Transmission," in *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, Apr. 2022, pp. 1987–1992, doi: 10.1109/WCNC51071.2022.9771838.
- [18] M. Rosecký, J. Pluskal, and R. Šomplák, "Network flow problem heuristic reduction using machine learning," *Optimization and Engineering*, vol. 25, no. 1, pp. 93–119, Mar. 2024, doi: 10.1007/s11081-023-09838-4.
- [19] M. Paricherla, M. Ritonga, S. R. Shinde, S. M. Chaudhari, R. Linur, and A. Raghuvanshi, "Machine learning techniques for accurate classification and detection of intrusions in computer network," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 4, pp. 2340–2347, Aug. 2023, doi: 10.11591/eei.v12i4.4708.
- [20] Z. Tafa and V. Milutinovic, "The Emerging Internet Congestion Control Paradigms," in *2022 11th Mediterranean Conference on Embedded Computing (MECO)*, Jun. 2022, pp. 1–5, doi: 10.1109/MECO55406.2022.9797207.
- [21] R. Ritzkal *et al.*, "K-nearest neighbor algorithm analysis for path determination in network simulation using software defined network," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 4, pp. 2388–2400, Aug. 2023, doi: 10.11591/eei.v12i4.4868.
- [22] M. Z. U. Haq *et al.*, "An Adaptive Topology Management Scheme to Maintain Network Connectivity in Wireless Sensor Networks," *Sensors*, vol. 22, no. 8, p. 2855, Apr. 2022, doi: 10.3390/s22082855.
- [23] W. Fan, F. Xiao, L. Han, X. He, and J. Wang, "Joint Optimization of Measurement Point Intelligent Selection and End-to-End Network Traffic Calculation in Datacenters," *IEEE Transactions on Network Science and Engineering*, pp. 1–12, 2024, doi: 10.1109/TNSE.2023.3278680.
- [24] Y. A. Farrukh, S. Wali, I. Khan, and N. D. Bastian, "SeNet-I: An approach for detecting network intrusions through serialized network traffic images," *Engineering Applications of Artificial Intelligence*, vol. 126, p. 107169, Nov. 2023, doi: 10.1016/j.engappai.2023.107169.
- [25] F. Zola, L. Seguro-Gil, J. L. Bruse, M. Galar, and R. Orduna-Urrutia, "Network traffic analysis through node behaviour classification: a graph-based approach with temporal dissection and data-level preprocessing," *Computers & Security*, vol. 115, p. 102632, Apr. 2022, doi: 10.1016/j.cose.2022.102632.
- [26] G. Mehmood, M. Z. Khan, A. K. Bashir, Y. D. Al-Otaibi, and S. Khan, "An Efficient QoS-Based Multi-Path Routing Scheme for Smart Healthcare Monitoring in Wireless Body Area Networks," *Computers and Electrical Engineering*, vol. 109, p. 108517, Jul. 2023, doi: 10.1016/j.compeleceng.2022.108517.
- [27] T. H. H. Aldhyani, M. Alrasheedi, A. A. Alqarni, M. Y. Alzahrani, and A. M. Bamhdi, "Intelligent Hybrid Model to Enhance Time Series Models for Predicting Network Traffic," *IEEE Access*, vol. 8, pp. 130431–130451, 2020, doi: 10.1109/ACCESS.2020.3009169.
- [28] D. A. Bierbrauer, M. J. De Lucia, K. Reddy, P. Maxwell, and N. D. Bastian, "Transfer learning for raw network traffic detection," *Expert Systems with Applications*, vol. 211, p. 118641, Jan. 2023, doi: 10.1016/j.eswa.2022.118641.
- [29] S. B. Klenow, C. Williamson, M. Arlitt, and S. Keshvadi, "Campus-Level Instagram Traffic: A Case Study," in *2019 IEEE 27th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, Oct. 2019, pp. 228–234, doi: 10.1109/MASCOTS.2019.00032.




- [30] F. C.-Rodríguez, M. L.-Gudiño, L. S.-Zambrano, and M. D.-Limaico, "Offensive Security: Ethical Hacking Methodology on the Web," *Advances in Intelligent Systems and Computing*, vol. 884, pp. 127–140, 2019, doi: 10.1007/978-3-030-02828-2_10.
- [31] C. Douligieris, S. Mitropoulos, and V. Toulas, "A prototype network monitoring information system: modelling, design, implementation and evaluation," *International Journal of Information and Communication Technology*, vol. 21, no. 2, pp. 111–136, 2021, doi: 10.1504/IJICT.2021.10042018.
- [32] Y. He, Y. Yang, B. Zhao, Z. Gao, and L. Rui, "Network Traffic Prediction Method Based on Multi-Channel Spatial-Temporal Graph Convolutional Networks," in *2022 IEEE 14th International Conference on Advanced Infocomm Technology (ICAIT)*, Jul. 2022, pp. 25–30, doi: 10.1109/ICAIT56197.2022.9862813.

BIOGRAPHIES OF AUTHORS






Nor Paezah Abdullah    is currently pursuing her Ph.D. in Electrical Engineering at Universiti Teknologi MARA (UiTM), Shah Alam, Selangor Malaysia. She is a Head of Department of Information Technology and Lecturer in the Diploma Computer Technology Program at the Institut Kemahiran Tinggi PERDA (PERDA-TECH). She received her Diploma in Computer Science in 2000 from Universiti Teknologi Mara (UiTM) Malaysia, her BSc (Hons) in Information Technology in 2012, and her M.Sc. in Education in 2015 from the Open University Malaysia (OUM), Malaysia. She has experience in teaching PC maintenance hardware and software, networking, telecommunications, cybersecurity, IoT, and project management during her services for 21 years. She is currently one of the trainers for the Cisco Networking Academy Program in Malaysia and an instructor for Cisco Networking Academy Malaysia since 2010 and a member of the Malaysian Board of Technology (MBOT). She can be contacted at email: Paezah79@gmail.com.






Assoc. Prof. Ts. Dr. Murizah Kassim    currently working as the Head of Publication and Innovation and Senior Fellow at the Institute for Big Data Analytics and Artificial Intelligence (IBDAAI), Universiti Teknologi MARA, Shah Alam. She is an Associate Professor from the School of Electrical Engineering, College of Engineering, Universiti Teknologi MARA. She received her Ph.D. in Electronic, Electrical, and System Engineering in 2016 from the Faculty of Built Environment and Engineering, Universiti Kebangsaan Malaysia (UKM). She has published many indexed papers related to computer networks, data engineering, IoT, web, and mobile development applications research. She has experience of 19 years in the technical team at the Centre for Integrated Information Systems, UiTM. She is also a member of the Enabling Internet of Things Technologies (EIIoTT) research group UiTM. She joined the academic in January 2009 and is currently a member of MBOT, IEEE, IET, IAENG, and IACSIT organizations. She can be contacted at email: murizah@uitm.edu.my.



Assoc. Prof. Dr. Sayang Mohd Deni    is an Associate Professor in the School of Mathematical Science, College of Computing, Informatics and Media, UiTM. She earned her Ph.D. in Statistics from Universiti Kebangsaan Malaysia, Bangi, Selangor. Her research interests include statistical modeling and computing, particularly in the application of environmental and hydrological data. She is a member of the Research Initiative Group of Flood Control. She is a life member of the Malaysian Statistical Institute, Malaysian Mathematical Sciences Society, and Management Science/Operation Research Society of Malaysia. She can be contacted at email: sayan929@uitm.edu.my.



Assoc. Prof. Ts. Ir. Dr. Yusnani Mohd Yusoff    is an Associate Professor at the College of Engineering, Universiti Teknologi MARA, Shah Alam Malaysia. Her research areas focus on wireless sensor networks, trusted authentication, embedded security, and the internet of things. She is currently the President of Cisco Netacad Academy for Malaysia. She is also heading a research interest group, namely the Information, Security and Trusted Infrastructure Laboratory or InSTIL research group. She has authored and co-authored 43 indexed publications with a SCOPUS h-index of 8. She is currently a member of IEEE, IAENG, and the Board of Engineer Malaysia. Prior to joining Universiti Teknologi MARA, she worked as a Test Engineer at Solectron Technology Sdn Bhd, Pulau Pinang. Upon getting her Ph.D. she was appointed as Head of the Department of Computer Engineering followed by Deputy Dean Academic. She is currently focused on supervising postgraduate students and teaching Cisco Academy Courses. She can be contacted at email: yusna233@uitm.edu.my.