Network Performance Analysis Using Packets Probe for Passive Monitoring

Jawad Alkenani [1]*, Khulood Ahmed Nassar [2]
Email: Jawadalkenani@sa-uc.edu.iq[1], khulood.nassar@uobasrah.edu.iq[2]
[1] Department of Computer Science, Shatt Al-Arab University College, Basra, Iraq
[2] College of Computer Science and Information Technology, Computer Information Systems Department, University of Basrah, Basrah, Iraq

Keywords: GUI, Java, Network Performance, Packets Probe, Passive monitoring

Received: July 20, 2022

Measuring network performance is essential in computer networks, and benchmarking may not be effective for installation in peripheral devices, resulting in replacing those devices and thus increasing cost. In light of this, it is better to have a software system for the network to see its performance rather than the actual design. In this paper, we developed negative network tomography techniques to infer correlation-level aberrations such as excessive loss rates and delays from path-level measurements. Our system involves placing packet probes in passive monitoring devices on strategic links within the network to learn about network performance with the identification of missing and transmitted packets, and to keep the cost of monitoring and communications infrastructure low. A graphical user interface (GUI) represents provided a variety of data, metrics. this work can be a useful guide for network researchers or other programmers to analyze their networks and understand how to calculate network performance, where it has been compared to the network performance measurement and evaluation system (NPMES), the results of the system were the accuracy of 94%.

Povzetek: V članku je predstavljena pasivna tomografska metoda za ugotavljanje lastnosti omrežij.

1 Introduction

Network performance is the investigation and review of aggregate network information to describe the quality of services provided by the underlying computer network. It is a qualitative and quantitative process that evaluates and specifies the performance level of a network. Therefore, it aids a network administrator in analyzing, assessing, and enhancing network services[1]. Therefore, there is a need for advanced monitoring tools capable of measuring network performance indicators such as end-to-end delay and packet loss continuously [2]. To meet the severe criteria for network, these next-generation monitoring systems must not only detect network performance degradation immediately but also identify the main cause of service quality issues, and solve this problem, we designed a passive monitoring system based on the language java that is low-cost to calculate the network performance measure[3]. Our system includes deploying packet probes in passive monitoring devices on important network lines to learn about network performance and reduce monitoring and communications infrastructure costs to a minimum. This work is represented by an easy-to-use graphical user interface, and network researchers and other programmers can use it to examine their networks and learn how to calculate network performance indicators[4]. Furthermore, by enabling prompt resolution of network issues (e.g., routing traffic around a crowded link), these monitoring tools will play a critical role in ensuring service quality and minimizing service outages. Passive monitoring techniques, on the other hand, infer network performance by eavesdropping on existing traffic crossing network lines[5]. Passive monitoring provides many advantages. First, it does not burden the network infrastructure with additional synthetic traffic for monitoring purposes. This is particularly important when a network interface or link becomes crowded, as injecting additional traffic for active measurements would simply exacerbate the problem. Second, since all measurements are based on actual network traffic, passive techniques may precisely evaluate the network performance end-users experience[6], [7].

In light of this, the monitoring system has now taken center stage in network application and design. Based on an in-depth analysis of the primary network QoS techniques. The performance evaluation standards based on performance aggregation and the prototype implementation of Network Performance Measurement And Evaluation System (NPMES) are carefully introduced. introducing new performance evaluation standards for accessing QoS that are based on performance aggregation. Results from the experiments show that scalable NPMES is capable of real-time detection of ISP network performance from the viewpoint of the end user. Where this system was slow with medium accuracy in the evaluation of performance measurement[8].

Table 1: Summarization Table on the Related Works.

Ref	Methodology	Performance/Results
[19]	• Passive Thermal Probes	• The proposed work aims to present the technique of passive thermal probes (PTPs) in its entirety. They have included an explanation of the design along with different calibration and evaluation methods, Exemplary experimental results were provided to emphasize its versatility and significance as a diagnostic for modern atmospheric pressure plasma research.
[20]	• Window of Transmission Control Protocol	• Several researchers have highlighted Quality monitoring and network performance evaluation to improve healthcare for patients to minimize delay and packet loss. • The network measurement was calculated based on the Congestion Window of Transmission Control Protocol. The analysis of all parameters is calculated based on the output of the simulator. However, the proposed study doesn't show the network format supported and the statistical results are calculated in external tools.
[21]	• Operating System Fingerprinting	• The field of static networks and managed environments is well-known for its operating system fingerprinting techniques. However, there aren't many studies that address this issue in actual networks where users can connect any device. With the help of a sizable dataset gathered from a university wireless network, we compare the effectiveness of three OS fingerprinting techniques. • The findings indicate that the most accurate method, which can only identify a small portion of the traffic, is one based on HTTP User-agents.
[22]	• Multipoint Passive Monitoring	• This work suggests a brand-new, non-intrusive, and adaptable technique for passively monitoring significant backbone networks. We can precisely measure packet losses in various network segments, only affecting specific flows, by using packet counters, which are readily available on current hardware. Not only end-to-end flows but any general flow with packets taking a number of different routes through the network can be observed (multipoint flows).
[23]	• Grid connectivity	• Present a scalable and non-intrusive method for determining the packet loss ratio between various measurement points that is based on passive network monitoring. • The suggested method can be easily incorporated into the network monitoring components of Grid systems and is a complement to the current active monitoring techniques. the present experimental evaluation results, including measurements with actual Grid application traffic, outline the design and implementation of the technique, sketch out its integration within a Grid environment.
[24]	• Smartphone Wi-Fi Probes	• dynamic fingerprint management plan and the smartphone's passive Wi-Fi probe, suggest a positioning algorithm. A person may have zero, one, two, or more smartphones with different Wi-Fi signals during actual public social activities. In order to determine the population, devise a method for calculating the likelihood of a user producing one Wi-Fi signal. put forth a method for estimating crowd density based on the positioning of Wi-Fi probe packets. • The proposed solution's ability to precisely and effectively estimate crowd density has been demonstrated through experiments carried out in three public social events as well as an indoor laboratory classroom.
[25]	• Passive Simple Network Measurement Protocol	• The measurement technique that was employed to collect the data shouldn't slant empirical analysis of Internet traffic characteristics. This paper compares probe-based (active) and router-based (passive) methods for measuring packet loss in a wide-area network as well as in a lab. • The wide-area experiments reveal that active-probe loss-rate measurements do not correlate with those obtained by SNMP from routers in a real network, despite the laboratory case study showing the accuracy of passive SNMP measurements at low loss rates.
[26]	• PMS-EN	• In order to manage performance in the context of enterprise networks, this work has described a new performance measurement system called PMS-EN. It offers businesses operating in this environment a straightforward, effective, reliable, and practical framework. Additionally, it fills a gap in most existing frameworks by providing an efficient and effective tool for developing, managing, and monitoring performance measures in a graphical and analytical manner at both the global and individual levels of the enterprise networks.
[8]	• NPMES	• The performance evaluation standards based on performance aggregation and the prototype implementation of NPMES are carefully introduced. introducing performance evaluation standards for QoS that are based on performance.

Table 1, shows the Summarization of the Related Works. In this work, we study the problem of designing a low-cost passive monitoring system to compute a network performance metric with the identification of missing and transmitted packets. The proposal is presented through a graphical user interface (GUI) provided along with a variety of data, metrics, and statistics related to network results.

This paper is organized as follows: In Section 2 presents the Passive network measurement. Section 3 describes a suggested system for analyzing packet probes using Java. It represents the process of analyzing the system and the interface of network performance with performance evaluation. Finally, the conclusion of this paper is presented in Section 4.

2 Passive Monitoring Measurement

Passive network measurement is based on the collection and analysis of traffic data to estimate network characteristics and evaluate observed network performance and behavior[9],[10]. The obtained data can be categorized as follows. As depicted in Figure 1, traffic is collected immediately and data and analytics are acquired via preprocessed devices. Depending on the collected data, passive monitoring can generate many unique outcomes. The fundamental advantage of passive measuring is that it does not interfere with the examined network. Using a Switched Port Analyzer Network, it is often possible to gather traffic from routers and switches without interfering with production traffic[7]. In this work, we use the most popular metrics related to performance analysis [11], [12].

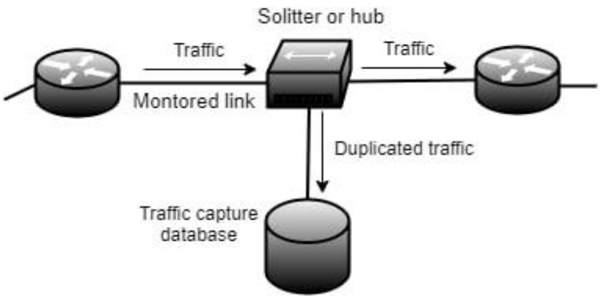

Figure. 1: Passive monitoring measurement [9]

The majority of modern devices contain a passive measurement mechanism, such as Remote Monitoring Networking (RMON), that can be used to collect data from the devices, including the number of bytes exchanged, packets lost, and other interface information. Typically, these built-in solutions produce highly aggregated data and offer little insight into the network state or traffic pattern. Typically, data created by these techniques can be retrieved via the Simple Network Management Protocol (SNMP). Ethereal and Wireshark, often known as Wireshark, are two of the most commonly used passive measuring tools. There are a few advantages of passive measurements over active measurements[13]. Given that passive techniques generate no new traffic, they do not interrupt the network and accurately describe network activity [14]. The passive measurement analyzes captured packet traces to identify network traffic. Passive measurement, in contrast to active measurement, does not put misleading traffic into the network. It only observes the network without producing or modifying actual network traffic. Increasingly, network operators and scholars in the networking industry depend on passive monitoring metrics[15].

Controlling the injected signal enhances noise reduction using passive monitoring measurement. The active procedure requires more time and labor than the passive experiment. In addition, varied source-receiver configurations provide diverse survey strategies. Increasing the number of field possibilities would raise review design costs and the probability of field mistakes. Moreover, the vast amount of data collected by modern clinical studies[6], [16].

3 Proposed Methods

In this proposal, we have developed negative network tomography techniques to infer correlation-level aberrations such as excessive loss rates and delays from path-level measurements. Our system includes deploying packet probes in passive monitoring devices on important network lines to learn about network performance and reduce monitoring and communications infrastructure costs to a minimum. This work is represented by an easy-to-use graphical user interface, and network researchers and other programmers can use it to examine their networks and learn how to calculate network performance indicators. Furthermore, by enabling prompt resolution of network issues (e.g., routing traffic around a crowded link), these monitoring tools will play a critical role in ensuring service quality and minimizing service outages.

One of the most important monitoring tools is the probe, which has many meanings:1) In telecommunications, a probe is an activity or device used to gather information on the status of a network. For instance, an empty message can be sent to determine if the recipient exists. 2) A probe is software or other device that is put at a critical network node to monitor or gather data regarding network activities. 3) In terms of network computer security, a probe is an effort to acquire access to a computer and its contents by exploiting a known or likely vulnerability in the computer system. 4) In the testing of semiconductors, a probe card is a microchip inserted into a circuit to examine its signals[17], [18].

The reason we need sensors for network monitoring is that network sensors conduct the laborious work of gathering information about a particular device's performance so that you don't have to. As long as you establish alerts to notify you of connected concerns, you may prioritize other information technology tasks. Network investigations will continue to poll your devices in the background and will collaborate with your monitoring solution to notify you if something goes wrong. Using sensors to monitor the network prevents bottlenecks, slowdowns, and downtimes that can cut daily operations in half. With the capacity to gather and receive near-real-time information about the network at an incredible rate, network probes retain up-to-date information, allowing you to be the first to identify any network issues and take appropriate action.

3.1 Design System

The system design is based on the Java language. This system is a graphical interface that researchers can make modifications to in the future. This interface contains 6 nodes to represent that system, as shown in figure 2.

The packets are sent through the best path, where the best path represents the shortest path from the source to the target, when sending packets through a specific path If the network is exposed to high congestion that leads to a deterioration of performance, the benefit of the probe is to know the number of lost and forwarded packets in the network to evaluate its performance. In this system, we use probe mode to find out the missing packets. In addition, metrics can be extracted to know the performance of the network.

3.2 Network Performance Interface

This section displays the network performance interface. The user can access and use this interface by selecting the node number of nodes, ranging from (N1 to N6), there is an input label below each node, as shown in Figure 3, which represents the amount of distance from one node to another. Then the number of transmitted packets is selected, and then "Draw" is selected, and the best path is drawn (the shortest path from the source to the target). Thus, the network can be exposed to congestion or interruption in the service, which leads to many packets being dropped.

This system provides the ability to determine the number of lost packets sent well, as shown in Figure 4. In addition, the menu displays the network performance interface for packets probe results, as shown in Figure 5. This set of interface contents is from the text box to enable the user to enter network parameters such as throughput rate, useful data capacity, jitter, etc.

The network performance makes it possible to forecast system behavior using a different variable. In every instance, the idea is that the simulation is a different realization that roughly approximates the system, and in every instance, the simulation's goal is to examine and comprehend how the system will behave in the face of various alternative courses of action or decisions. This field can identify more precise requirements that might be used in the real system because it is more focused than a real system. Before applying these features to the actual system, the researchers might, for instance, concentrate on the network's effectiveness and validity and present the results. All of the statistical network data can be displayed thanks to this user interface.

Throughput refers to the quantity of data moving across the network from one point to another within a specified time. When referring to communication networks, throughput is the rate of data that was successfully transmitted via a communication channel. The standard unit of measurement for network throughput is bits per second (bits/s or bps). Network congestion happens when network devices are unable to deliver the comparable quantity of traffic they receive, thus their packet buffer fills up and they start losing packets. If there are no disruptions on the network at an endpoint, every packet will arrive. However, as the endpoint buffer grows full, packets arrive later and later. Goodput is less than throughput (the gross bit rate that is physically transferred), which is often less than the network access connection speed.

Delay is the measurement of how long it takes for data to reach its destination over a network. Typically, network latency is measured as a round-trip delay in milliseconds (ms), taking into account the time it takes for data to travel from its source to its destination and back again.

3.3 Evaluation System

The proposed network monitoring system can be used in real networks' performance evaluations, and it enables experts to review the result due to the simplicity of the graphical representation. In this way, the proposed system provides a deep insight into the network factors that lead to determining the glitch. For example, in the network, many metrics affect service quality. Therefore, finding the specific factor is very important and can assist in the enhancement of the quality of service. This research has treated the problem of multiple networks' evaluations based on the most common metrics for monitoring service quality. The traditional monitoring system has focused on each single network analysis independently. In this research, the idea of multiple analyses of networks' quality of service has been presented to find the optimal network.

This interface can display the network performance result for all the metrics at the same time, the user has to select the source node, the destination node, and the packet size and then select one of the metrics that the user wants to calculate and then press the “Ran” button and based on that, the system will display the result depending on required value. Where it has been compared to the Network Performance Measurement and Evaluation System (NPMES), the results of the system were the accuracy of 94%.

The figure 6 shows the result of the accuracy of the system.

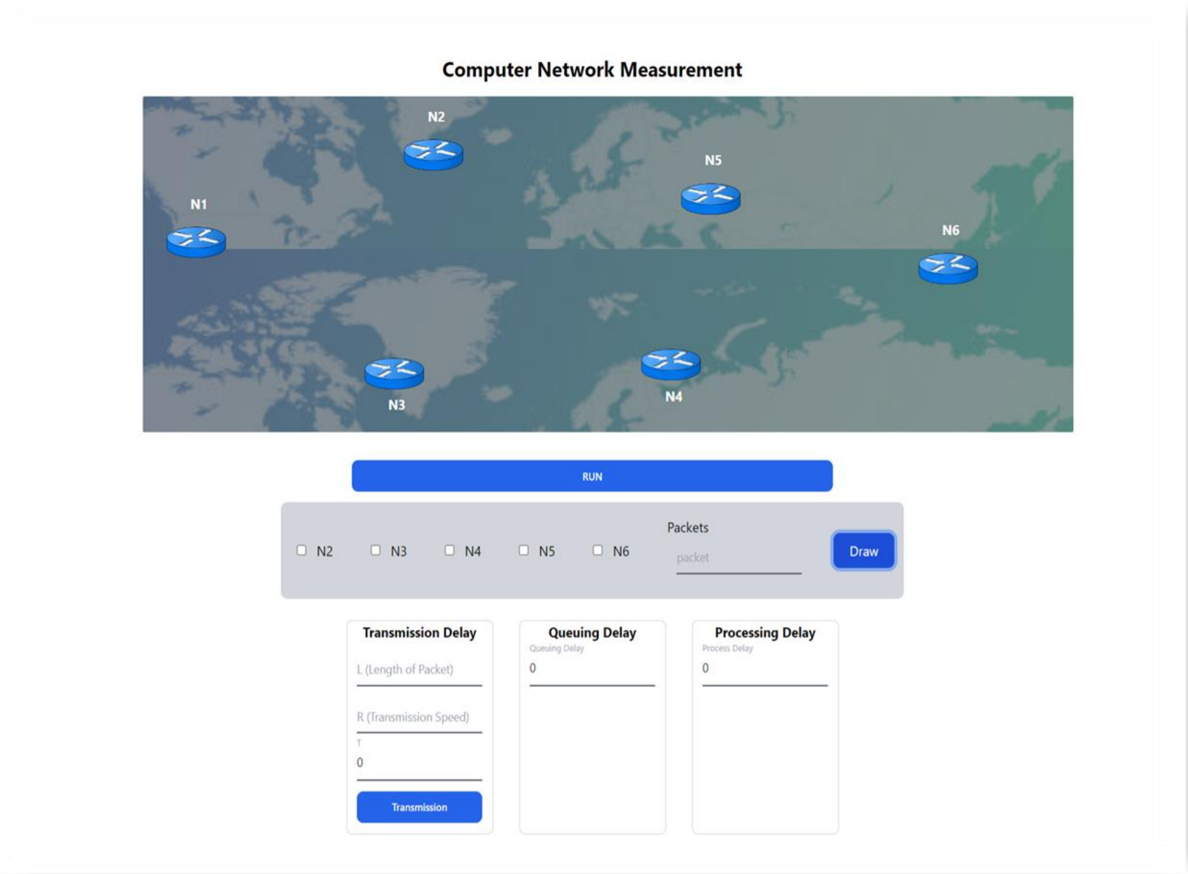

Figure 2: The System Design Performance of the Network

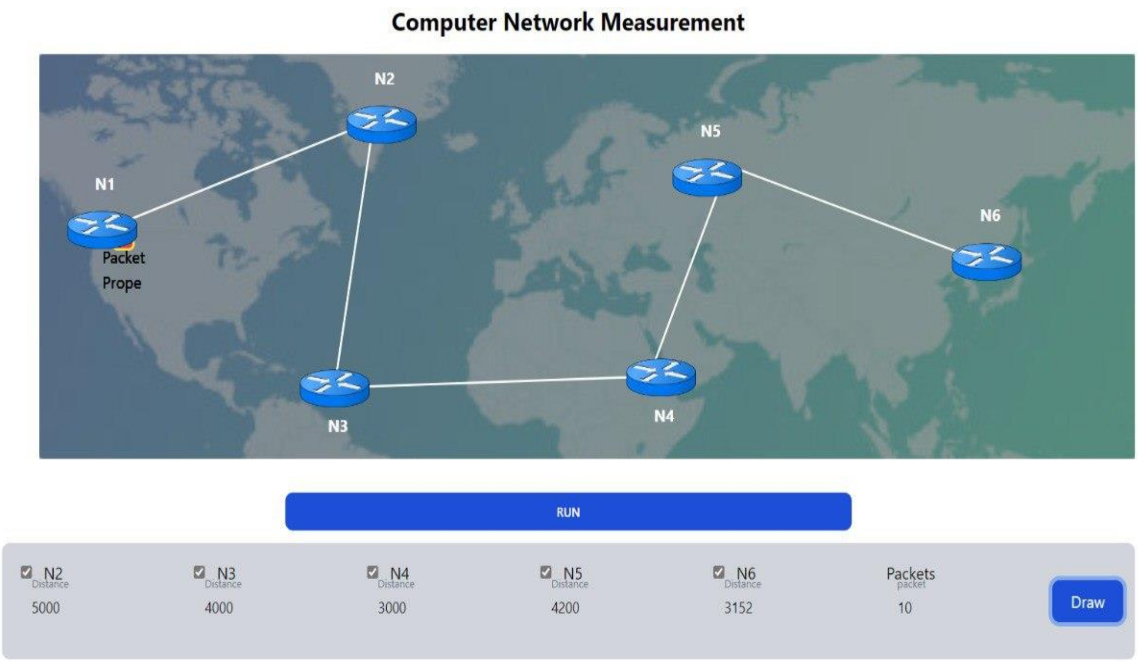

Figure 3: Input Parameters of the Network

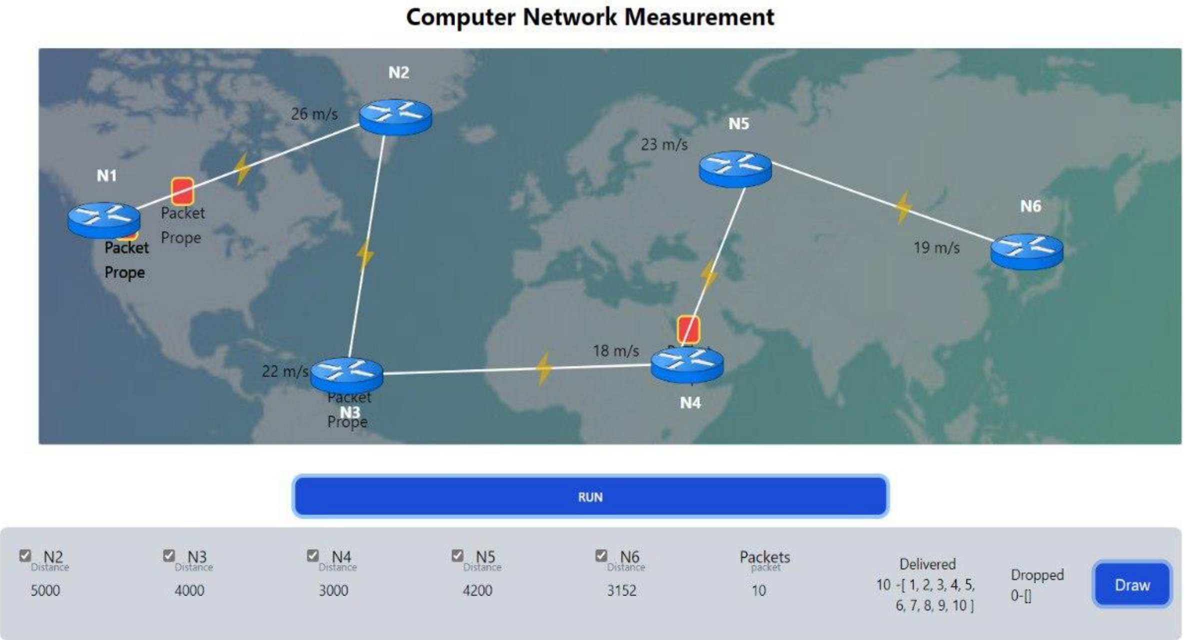

Figure 4: Dropped Packets of the Network

Measurements

NODE	PACKET PROPE										
	PACKET 1	PACKET 2	PACKET 3	PACKET 4	PACKET 5	PACKET 6	PACKET 7	PACKET 8	PACKET 9	PACKET 10	AVRAGE PACKET PROP
N2	26	26.1	26.2	26.3	26.4	26.5	26.6	26.7	26.8	26.9	26.45
N3	22	22.1	22.2	22.3	22.4	22.5	22.6	22.7	22.8	22.9	22.45
N4	18	18.1	18.2	18.3	18.4	18.5	18.6	18.7	18.8	18.9	18.45
N5	23	23.1	23.2	23.3	23.4	23.5	23.6	23.7	23.8	23.9	23.45
N6	19	19.1	19.2	19.3	19.4	19.5	19.6	19.7	19.8	19.9	19.45
End to End Delay	108	108.1	108.2	108.3	108.4	108.5	108.6	108.7	108.8	108.9	108.45
Jitter	10.78 m/s			Throughput					13.89 m/s		
Delay	108.45 m/s			Goodput					8.49 m/s		

RUN

Figure 5: Packets Probe Result

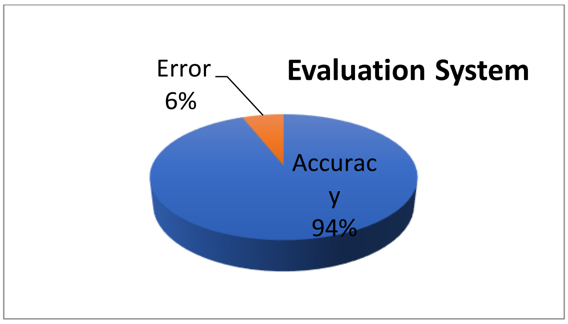

Figure 6: Accuracy of the System.

5 Conclusion

In this work, we designed a Java-based software system for the passive network to infer correlation-level aberrations such as excessive loss rates and delays from passive monitoring beam probe measurements. the system involves placing packet probes in passive monitors on strategic links within the network to learn about network performance while identifying lost and sent packets, and to keep the cost of monitoring and communication infrastructure low. This work is represented by an intuitive graphical user interface (GUI) that is provided along with a variety of data, metrics, and statistics related to network results, where which has been compared to the Network Performance Measurement and Evaluation System (NPMES). The result of the proposed system was accuracy of 94%. and this work can be a useful guide for network researchers or other programmers to analyze their networks and avoid errors in them. This system is fast and highly accomplished. Future work, calculating various metrics and statistics with 3D interfaces to visualize the state of the network.

References

[1] L. Ye *et al.*, "PUFF: A Passive and Universal Learning-based Framework for Intra-domain Failure Detection," in *2021 IEEE International Performance, Computing, and Communications Conference (IPCCC)*, pp. 1–8, 2021, https://doi.org/ 10.1109/IPCCC51483.2021.9679436.

[2] M. Abbasi, A. Shahraki, and A. Taherkordi, "Deep learning for network traffic monitoring and analysis (NTMA): A survey," *Comput. Commun.*, vol. 170, pp. 19–41, 2021. https://doi.org/10.1016/j.comcom.2021.01.021

[3] A. Salama and R. Saatchi, "Probabilistic classification of quality of service in wireless computer networks," *ICT Express*, vol. 5, no. 3, pp. 155–162, 2019, https://doi.org/10.1016/j.icte.2018.09.001.

[4] R. A. Osman, X. H. Peng, M. A. Omar, and Q. Gao, "Quality of service optimisation of device-to-device communications underlaying cellular networks," *IET Commun.*, vol. 15, no. 2, pp. 179–190, 2021, https://doi.org/10.1049/cmu2.12040.

[5] Y. He and X. Zhang, "A Survey on Network Measurement for Software-Defined Networks," in *2019 3rd International Conference on Electronic Information Technology and Computer Engineering (EITCE)*, pp. 1534–15402019, https://doi.org/10.1109/EITCE47263.2019.9095170.

[6] P. Manzanares-Lopez, J. P. Muñoz-Gea, and J. Malgosa-Sanahuja, "Passive in-band network telemetry systems: The potential of programmable data plane on network-wide telemetry," *IEEE Access*, vol. 9, pp. 20391–20409, 2021, https://doi.org/10.1109/ACCESS.2021.3055462.

[7] D. Perdices, D. Muelas, L. de Pedro, and J. E. L. de Vergara, "Network performance monitoring with flexible models of multi-point passive measurements," in *2018 14th International Conference on Network and Service Management (CNSM)*, pp. 1–9, 2018.

[8] S. Hongjie, F. Binxing, and Z. Hongli, "A distributed architecture for network performance measurement and evaluation system," in *Sixth International Conference on Parallel and Distributed Computing Applications and Technologies (PDCAT'05)*, pp. 471–475, 2005, https://doi.org/10.1109/PDCAT.2005.8

[9] J. Alkenani, K. A. Nassar, I. Technology, and C. Information, "Network Monitoring Measurements for Quality of Service : A Review," no. May, 2022, https://doi.org/10.37917/ijeee.18.2.5 ,

[10] I. S. Alshawi, Z. A. Abbood, and A. A. Alhijaj, "Extending lifetime of heterogeneous wireless sensor networks using spider monkey optimization routing protocol," *Telkomnika*, vol. 20, no. 1, 2022, http://doi.org/10.12928/telkomnika.v20i1.20984.

[11] K. A. Nassar and A. A. Abdullah, "End-to-End Fuzzy RED to Reduce Packet Loss in Virtual Circuit Network," *J. Univ. Babylon*, vol. 25, no. 3, 2017.

[12] B. Constantine, G. Forget, R. Geib, and R. Schrage, "Framework for TCP throughput testing," *Internet Eng. Task Force*, vol. 2011, pp. 1–27, 2011, http://doi.org/10.17487/RFC6349.

[13] V. Mohan, Y. R. J. Reddy, and K. Kalpana, "Active and Passive Network Measurements : A Survey," *Comput. Sci. Inf. Technol.*, vol. 2, no. 4, pp. 1372–1385, 2011, http://doi.org/10.19865/45886349.

[14] D. Perdices, D. Muelas, I. Prieto, L. de Pedro, and J. E. L. de Vergara, "On the modeling of multi-point RTT passive measurements for network delay monitoring," *IEEE Trans. Netw. Serv. Manag.*, vol. 16, no. 3, pp. 1157–1169, 2019, http://doi.org/ 10.1109/TNSM.2019.2924812.

[15] D. H. Hagos, P. E. Engelstad, A. Yazidi, and Ø. Kure, "General TCP state inference model from passive measurements using machine learning techniques," *IEEE Access*, vol. 6, pp. 28372–28387, 2018,http://doi.org/10.1109/ACCESS.2018.2833107 .

[16] E. Browning, R. Gibb, P. Glover-Kapfer, and K. E.

Jones, "Passive acoustic monitoring in ecology and conservation,"2017,http://dx.doi.org/10.25607/OBP-876.

[17] A. G. Castro *et al.*, "Near-optimal probing planning for in-band network telemetry," *IEEE Commun. Lett.*, vol. 25, no. 5, pp. 1630–1634, 2021, http://doi.org/10.1109/LCOMM.2021.3053485.

[18] T. Hou, T. Wang, Z. Lu, and Y. Liu, "Combating adversarial network topology inference by proactive topology obfuscation," *IEEE/ACM Trans. Netw.*, vol. 29, no. 6, pp. 2779–2792, 2021, http://doi.org/ 10.1109/TNET.2021.3101692.

[19] L. Rosenfeldt, L. Hansen, and H. Kersten, "The Use of Passive Thermal Probes for the Determination of Energy Fluxes in Atmospheric Pressure Plasmas," *IEEE Trans. Plasma Sci.*, vol. 49, no. 11, pp. 3325–3335,2021,http://doi.org/10.1109/TPS.2021.3092752

[20] S. H. Shetty, "Trace File Analysis To Obtain Congestion Window, Throughput And PDR," *Eur. J. Mol. Clin. Med.*, vol. 7, no. 08, p. 2020.

[21] M. Lastovicka, T. Jirsik, P. Celeda, S. Spacek, and D. Filakovsky, "Passive os fingerprinting methods in the jungle of wireless networks," in *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*, pp. 1–9, 2018, http://doi.org/10.1109/NOMS.2018.8406262.

[22] M. Cociglio, G. Fioccola, G. Marchetto, A. Sapio, and R. Sisto, "Multipoint passive monitoring in packet networks," *IEEE/ACM Trans. Netw.*, vol. 27, no. 6, pp. 2377–2390, 2019, http://doi.org/10.1109/TNET.2019.2950157.

[23] A. Papadogiannakis, A. Kapravelos, M. Polychronakis, E. P. Markatos, and A. Ciuffoletti, "Passive end-to-end packet loss estimation for grid traffic monitoring," in *Proceedings of the CoreGRID Integration Workshop*, pp. 79–93, 2006,

[24] X. Tang, B. Xiao, and K. Li, "Indoor crowd density estimation through mobile smartphone wi-fi probes," *IEEE Trans. Syst. man, Cybern. Syst.*, vol. 50, no. 7, pp.2638–2649, 2018, http://doi.org/10.1109/TSMC.2018.2824903.

[25] P. Barford and J. Sommers, "Comparing probe-and router-based packet-loss measurement," *IEEE Internet Comput.*, vol. 8, no. 5, pp. 50–56, 2004, http://doi.org/10.1109/MIC.2004.34.

[26] J. José Alfaro Saiz, A. Ortiz Bas, and R. Rodríguez Rodríguez, "Performance measurement system for enterprise networks," *Int. J. Product. Perform. Manag.*, vol. 56, no. 4, pp. 305–334, Jan. 2007, https://doi.org/10.1108/17410400710745324.