Received: 4 April 2022 | Revised: 4 May 2022 | Accepted: 5 May 2022
DOI: 10.37917/ijeee.18.2.5 Vol. 18| Issue 2| December 2022

Open Access

Iraqi Journal for Electrical and Electronic Engineering
Review Article

IJ EEE University of Basrh College of Engineering

Network Monitoring Measurements for Quality of Service: A Review

Jawad Alkenani*[1,2], Khulood Ahmed Nassar[1]
[1] College of Computer Science and Information Technology, Computer Information Systems Department, University of Basrah, Basrah, Iraq
[2] Department of Computer Science, Shatt Alarab University College, Basrah, Iraq

Correspondence
* **Jawad Alkenani**
Computer Information Systems Department
University of Basrah, Basrah, Iraq
Email: Jawadalkenani@sa-uc.edu.iq
khulood.nassar@uobasrah.edu.iq

Abstract

One crucial challenge confronting operators worldwide is how to ensure that everything runs smoothly as well as how to monitor the network. The monitoring system should be accurate, easy to use, and quick enough to reflect network performance in a timely way. Passive network monitoring is an excellent tool for this. It could be used to look for issues with a single network device or a large-scale issue affecting the whole LAN or core network. However, passive network monitoring is not limited to issue resolution; it could also be used to generate network statistics and measure network performance. As shown in this review, it is a very strong tool, as seen by the sheer volume of data published on Google Scholar. The main objective of this review is to analyze and comprehend monitoring measurements for quality of service to serve as a resource for future research and application. Essential terms and concepts of network monitoring and their quality of service are presented. Network monitoring measurements (which can be passive, active, or hybrid) and their wireless network monitoring tools (which can be public domain or commercial tools) are also covered in terms of relevance, advantages, and disadvantages. Finally, the review is summarized.

Keywords: Active Monitoring, Hybrid Monitoring, Passive Monitoring, Quality of Service, Tools Monitoring Wireless Networks.

I. Introduction

Millions of computers and computer users are connected through computer networks globally. The network has evolved into infrastructure for various applications that touch every aspect of our lives. Therefore, maintaining a well-maintained computer network is critical. Network management requires surveillance. Network monitoring involves a set of technologies that allow network administrators to assess the health of an extensive computer network [1]. Network monitoring is a set of strategies used for ensuring the security and integrity of an internal network. Internal networks are sometimes referred to as local area networks. Monitoring encompasses hardware, software, viruses, spyware, vulnerabilities, backdoors and security flaws, and other elements that may threaten the integrity of a network. Network monitoring is a time-consuming and complicated process integral to a network administrator's job. Network managers are constantly working to maintain the seamless operation of their networks. When a network is offline for even a little while, productivity within a corporation is affected. In the case of public-sector organizations, the ability to provide critical services is threatened. Administrators must monitor network traffic flow and performance to be proactive rather than reactive. They must also ensure no security breaches within the network [2], [3].

When a network fails, monitoring agents are tasked with identifying, isolating, and correcting network defects and recovering from the failure. The agents should notify the administrators within a minute and direct them to resolve the issues. With a stable network, the administrator's responsibility remains ongoing monitoring for threats from inside or beyond the network. Additionally, they must evaluate network performance regularly to ensure that no network devices get overloaded, and can use network monitoring Measurements before a network collapses due to congestion [4]. In the literature, passive flow measurement and active network quality monitoring technologies are designed. Various service detection methods are available to check the quality of the distribution network service communication network in real-time [5], neural network modeling for wireless communication network monitoring

[6], and the traffic service profile on an integrated basis [7]. Monitoring could be passive, active, or hybrid. Passive network monitoring collects data without interfering with traffic flow. Active network monitoring allows the modification of data on the connection. Network Simulator NS-2 or OPNET software is used to simulate the network topologies, hybrid monitoring active, and passive measurements combined for an illustration of the effectiveness and efficiency of network monitoring [8-10]. This review provides basic network monitoring terminology, concepts, and tools (public domain or commercial tools) and a complete and valuable explanation of network-monitored procedures with the best metric (passive, active, or hybrid) based on important literature. It also presents a summary of the review.

This paper is organized as follows: Section 2 provides network monitoring essential terms and concepts. Section 3 discusses service quality. Section 4 further discusses the relevance and uses of network monitoring measurements, which could be passive, active, or hybrid. Section 5 contains tools for wireless network monitoring (public domain or commercial). Finally, Section 6 gives a conclusion of the study.

II. Essential Terms and Concepts

This section defines several fundamental words and concepts relating to computer networks, with general guidelines for users to network problem solutions [4], [3], [11].

A. *General Guidelines of Network Monitoring*

1) *Conduct an inventory of the business* **:**Accurate inventory of the network's devices and applications is taken. Solutions that can find devices automatically are utilized to save IT the time and effort associated with this process.

2) *Evaluate the magnitude and danger of proposed changes:* The network change management process is guided by best practices to minimize the chance of a failed change. Applying certain fundamental operational principles, such as assessing the breadth of a proposed change, can help avoid future blunders.

3) *Use the best network metrics***:** Network metrics, such as instability, packet loss, throughput, and reliability, are measured.

4) *Continuous Monitoring*: Continuous monitoring helps discover intermittent network faults that are difficult to pinpoint precisely.

B. *Essential Terms of Network Monitoring*

Monitoring the network is important to see how well it is performing, such as bandwidth usage, delay, and others. In this part, the most important basic network terms are introduced [12],[13].

1) *Path:* It is a collection of links in a network that connects a source node to a destination node. The nodes that link the connections would be part of the path's structure [14].

2) *Link capacity:* It is defined as the greatest transfer rate that could be achieved across that link [15]. The capacity of a connection is specified at the protocol layer level. While the physical connection is the same, the link capacity on Layers 2 and 3 is different, indicating that the physical link has a different capacity. As in (1), the capacity C of an end-to-end route is equal to the capacity C_i of the smallest link in the path.

$$C = \min C_i \qquad (1)$$

3) *Delay (latency):* It has several types in telecommunications, including processing delay, propagation delay, queue delay, and transmission delay, as in (2). The word "delay" in this work applies to all kinds of delays; thus, it is referred to as "end-to-end delay" [16], [17].

$$D_{E2E} = D_{\text{processing}} + D_{\text{transmission}} + D_{\text{propagation}} + D_{\text{queuing}} \qquad (2)$$

Processing delay is the total of the processing delays produced by all intermediary nodes along the network route. A router must evaluate the header of an incoming packet to decide where to route it. It does bit-level error checking to see whether the packet is faulty, and it would handle the packet by performing functions such as firewalling and encryption. All of these operations performed by the router contribute to processing latency. Processing delays happen primarily at the network's edge routers.

Transmission (or serialization) delay is the time required to send a packet at the connection's bit rate. Thus, transmission delay is the time it takes a router to transfer an entire packet through a connection as in (3).

$$D_{\text{transmission}} = L/R \qquad (3)$$

where L denotes the packet's length and R denotes the link's transmission rate.

Propagation delay is the time required for a signal to travel from one end of the transmission medium to the other. Given that delay is medium-dependent, it is defined as the distance between two endpoints divided by the propagation speed, as in (4).

$$D_{\text{propagation}} = d/\eta\, C \qquad (4)$$

where d is the distance, c is the speed of light, and $\eta \leq 1$.

Queuing delay is the time required for a packet to traverse a router's queue from the source to the destination node. The queuing time is proportional to the buffer size and the amount of cross-traffic entering the router.

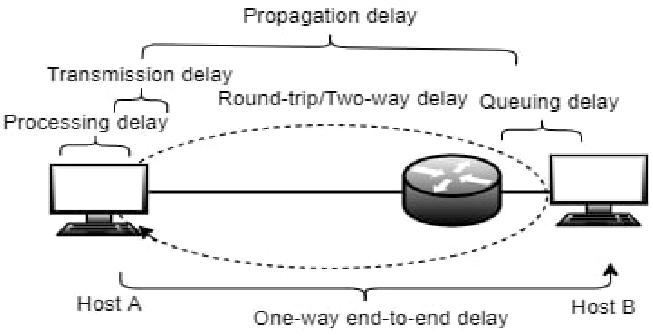

Fig. 1: Type of delay

Delay measures could be one-way or two-way. One-way delay quantifies the time required for a packet to transit between the transmitting and receiving hosts (Hosts A and B) in Fig. 1, the phrase "two-way delay" (or round-trip time, RTT) refers to the time required for a packet to go between the sender and the receiver and return.

4) *Jitter:* It is jittery. The term "variation" refers to the variance of packets' one-way delays (or jitter). The word is now deprecated because it has been used in various ways by various parties. The instantaneous packet delay variation may be determined using the one-way delays of two subsequent packets as in (5):

$$PDV_{Instantaneous} = D_{n+1} - D_{n} \qquad (5)$$

where D_{n+1} and D_n are one-way delays of two consecutive packets.

Delays can vary because of network congestion, routing changes, or timing drift. It is evident in real-time applications, such as VoIP or video streaming when jerky visual and audio breakdowns emerge. Buffering is used to alleviate the effects of delay variation. Packets are buffered and re-played at the receiving end of a VoIP connection after a short delay, aiding the receiver in arranging and spacing incoming packets to preserve as much of the original voice stream as possible.

Packet inter-arrival time variation refers to the time difference between packet arrivals at a host (also called a jitter). By comparing the arrival times of two successive packets, the instantaneous packet inter-arrival time can be determined as in (6):

$$IAT_{Instantaneous} = A_{n+1} - A_{n} \qquad (6)$$

where A_{n+1} and An are the arrival times of two consecutive packets.

5) *Queuing:* It refers to the technique used in packet networks to mitigate the effects of burst traffic. A router can only process one packet at a time. When packets arrive at a router faster than the router's capability for processing them, they are queued. Packets are queued until the router has enough processing time to process them. If the queue becomes full and further packets arrive, the router discards them, which is the main cause of packet loss [13].

6) **"***Packet loss," "loss time," and "loss distance"*: refer to when a packet is transferred from host A to host B but never reaches B, which is known as packet loss. Given that waiting forever for a packet is impractical, most networks have a timeout mechanism that discards the packet if reaching the other end of the network takes an unacceptable length of time. Even if a packet ultimately reaches B, it may be reported as lost [13],[18].

Packet loss can occur for several reasons: the router may delete a packet as a result of a buffer overflow or because the incoming packet is corrupted, or the packet may also be misrouted or lost as a result of a connection failure or wireless channel error. Packet loss can also be the result of malfunctioning or incorrectly designed equipment. Certain congestion management or avoidance algorithms (for example, Random Early Discard (RED)) can cause packet loss on purpose to drive Transmission Control Protocol (TCP) window size reductions.

Loss period and **loss** distance are two critical concepts that are inextricably linked to packet loss. The loss period is the number of consecutive packets lost during a packet loss event. The period begins with the loss of a packet and the receipt of the previous packet and concludes with the receipt of a packet and the loss of the preceding packet. The loss distance between two consecutively lost packets is the difference in their sequence numbers. They may have received packets in between.

7) *Throughput:* It refers to the quantity of data that a system can process in a certain amount of time. The edge nodes keep track of the number of packets and bytes delivered and received and the timestamps for each monitoring packet. Thus, determining the throughput (in bits per second) and the distribution of total outgoing traffic between receiving edge nodes is feasible. Peak rate resolution is proportional to the size of the monitoring block [19].

8) *Available bandwidth*: It is the capacity of a connection not in use for a certain period. Suppose Ci is the connection's capacity and ui is the link's average utilization (i.e., the link transmits Ciui bits) during time T. In that case, the link's available bandwidth is Ai, as in (7)[20]:

$$A_i = (1-u_i)C_i \qquad (7)$$

which yields the available bandwidth for an N-hop path as in (8):

$$A_i = \min A_i \quad ,i=1..N \qquad (8)$$

9) *Bulk Transfer Capacity (BTC) :* measure is defined as follows in (9)[21]:

$$BTC = \text{sent data bits/elapsed time} \qquad (9)$$

where sent data bits denote the number of unique data bits sent, unique in the sense that header bits and retransmissions are omitted. BTC is a unit of measurement used to describe the maximum possible throughput by a TCP or other congestion-aware transport protocol connection. Given that BTC is a TCP-specific metric, it cannot be compared with available bandwidth.

10) *Goodput*: It refers to the effective throughput experienced by a user, which may also be called application-level throughput. The term "goodput" refers to the rate at which a network or system can send user data bits per time unit (often seconds). One may determine goodput by deducting all header costs and retransmissions from throughput [22].

11) *Probes*: They are specialized probe packets that can be used for active measurements. A probe packet is a fictitious packet that can take on almost any shape to obtain desired data from the measurement. The network is probed, and the response is gathered and evaluated. A straightforward probe packet is a small UDP packet that carries just a timestamp and little or no data. This kind of probe could be used to determine the latency of VoIP systems or assess their performance.[13]

12) *Metrics*: A metric is a numerical value associated with the Internet's performance and dependability. It could

be considered a general indication of the network's performance. A single measurement result of a metric is referred to as a "singleton" metric, whereas a "sample" metric is a group of unique measurement results (singletons). Finally, a statistical metric is a metric that is constructed over a sample metric [23].

13) *Intrusiveness:* It is a feature of measurement equipment that indicates how much bandwidth it uses. Active measurement standards classify a tool or approach as invasive if the average probing load it places on the network during a measurement is disproportionate to the route's available bandwidth. Active network analysis uses a fraction of the available bandwidth and adds an extra burden to the observed network [24].

14) *Retransmission:* The rate informs the organization how often packets are lost, which is a sign of network congestion. Retransmission delay or the time required to retransmit a lost packet may be evaluated to determine how long the network takes to recover from packet loss [25].

15) *Connectivity:* It is a term that relates to the state of the connections between the nodes in the network. If the network has an inappropriate or dysfunctional connection, ideally, each link should operate at maximum capacity at all times. However, performance concerns such as malware may influence performance in a localized section of the network by targeting specific nodes or connections [26].

III. Quality of Service of a Network

The quality of service (QoS) refers to a network's capacity to handle a range of network performance levels that can be matched to the requirements of the applications supported by the network [27]. Figure 2 shows the most common metrics for monitoring service quality.

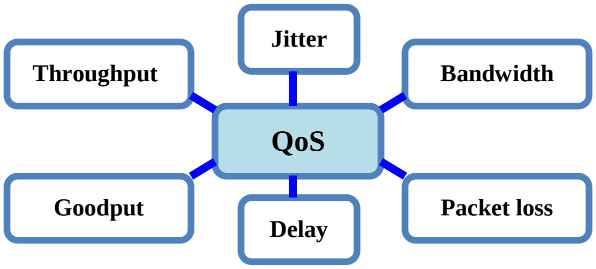

Fig. 2: Metrics for monitoring service quality

A. Importance for Quality of Service

QoS is most typically utilized in packet networks. Bandwidth, latency, and delay variation are not issues for circuit networks. In reality, a circuit network's basic nature is to maintain a steady bandwidth, low variance in latency, and the shortest overall delay. In terms of QoS, the circuit network is the gold standard for measuring packet networks [28], [29].

B. Advantages for Quality of Service

QoS is vital for firms seeking to assure the availability of mission-critical applications. It is critical for providing differentiated bandwidth and ensuring that data is sent without interfering with traffic flow or resulting in packet loss [30-34]. Several significant benefits of implementing QoS include the following:

1) *Preventing Packet loss*: Packet loss occurs when data packets are lost in transit between networks. It is often caused by network congestion, a broken router, a loose connection, or a bad signal. By prioritizing bandwidth for high-performance applications, QoS eliminates the possibility of packet loss.

2) *Reduced latency*: Latency refers to the amount of time it takes for a network request to go from the sender to the receiver and be processed by the receiver. It is often influenced by the additional time for routers to inspect data and the storage delays provided by intermediate switches and bridges. By prioritizing critical applications, QoS enables organizations to reduce latency and expedite network request processing.

3) *Prioritization of apps is unlimited*: QoS ensures that enterprises' most mission-critical applications are always given precedence and the resources required to function well.

4) *Enhanced user experience*: The ultimate purpose of QoS is to ensure the high performance of mission-critical applications, which is equivalent to an optimal user experience. Employees benefit from great performance on their high-bandwidth apps, which helps them be more productive and complete tasks faster.

5) *Unlimited prioritization of apps*: QoS ensures that enterprises' most mission-critical applications always get precedence and the resources are required to execute at a high level.

C. Disadvantages of Service Quality

1) *QoS prioritizing*: The disadvantage of QoS prioritizing is that it does not provide a consistent user experience. Prioritization based on the quality of service and the various components of the data path(s) may not always add to a whole user experience (quality experience).

2) *Restricted Availability of Resources*: Creating QoS provisioning is highly tough in networks. Security features lead to QoS challenges.

3) *Proactive and Reactive Routing:* Reactive routing is sluggish, but proactive routing is resource-intensive. Slow routing leads to additional delays, and the use of more resources depletes the device's processing power and battery life.

IV. Network Monitoring Measurements

Monitoring a network could be passive, active, or hybrid. Passive network monitoring gathers data from the connection without interfering with traffic flow. Active network monitoring includes the capability of editing the data on the line. A hybrid measurement uses active and passive measurement [13], [35].

A. Active Monitoring Measurements

Active measurement methods are built on the principle of introducing traffic into a network to obtain information about its properties. This technique can be used to acquire reliable data and estimate the quality of observed network segments either on large-scale networks, end-to-end or per link. On the one hand, active measures are inherently network-invasive. This property is undesirable in certain cases because the measurement traffic modifies the observed link behavior. On the other hand, in certain situations, QoS parameters must be precisely approximated for a specified period [13], as shown in Fig. 3.

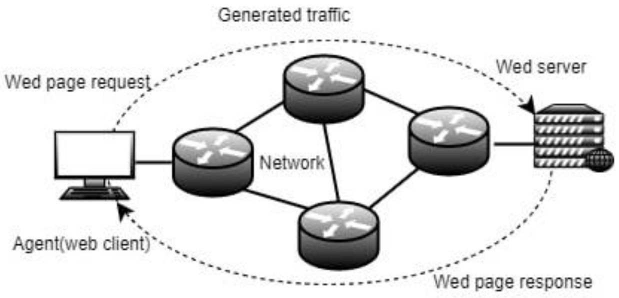

Fig. 3: Active monitoring measurements

Active measurement strategies include producing traffic and watching its behavior as it travels the network. The primary disadvantage of this strategy is that it is invasive, given that more traffic must be created. Such intrusiveness is sometimes useful, for example, when attempting to stress a network to define the presence of abused or accessible resources. Active approaches can be used to test and evaluate networks periodically. This method results in a stratification of the active measurement to describe the network behavior over time and concerning the network's state. Active approaches are primarily classified into two broad categories: file transfer/batch data transfer techniques and packet-pair techniques. This separation is made based on the technology used to create traffic and then analyze it to determine QoS metrics [36].

B. *Passive Monitoring Measurements*

The concept of passive network measurement is based on collecting and processing traffic data to estimate network characteristics and assess observed network performance and behavior. The data obtained can be classified as follows. Traffic is recorded directly, and data and analytics are acquired from devices that have been preprocessed, as shown in Fig. 4. Passive monitoring can provide a variety of distinct outputs based on the data obtained. The primary benefit of passive measurement is that the studied network is non-intrusive. Using a Switched Port Analyzer Network, traffic on routers and switches can typically be collected without interfering with production traffic [37].

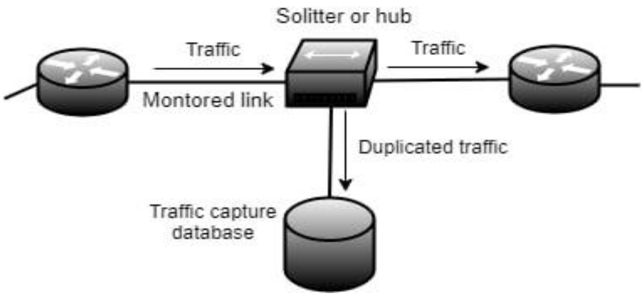

Fig. 4: Passive monitoring measurements.

The majority of current devices have some kind of passive measurement mechanism, such as RMON, that may be used to collect various sorts of data from the devices, such as the number of bytes transferred, packets lost, and other interface information. Typically, these built-in techniques provide highly aggregated data and give minimal information about the network condition or traffic pattern. Often, data generated by these methods can be retrieved using the SNMP protocol. Ethereal (affectionately known as Wireshark) and tcpdump are two of the most frequently used passive measurement tools. Passive measures have a few benefits over active measurements. Given that passive approaches generate no new traffic, they do not disrupt the network and give an accurate depiction of network traffic [13],[38].

C. *Hybrid Monitoring Measurements*

Hybrid measurement refers to active and passive measurements in conjunction with one another, as shown in Fig. 5. A hybrid measurement scenario is one in which active probes are distributed through a network, and their progress is passively monitored during the measurement. The measurer may then track the probes' passage and report their intermediate and end-to-end delays. This is not achievable with passive probing alone [13].

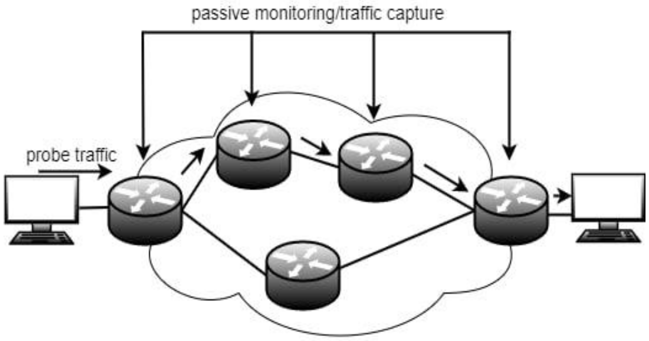

Fig. 5: Hybrid monitoring measurements

The case outlined needs the measurer to have administrative access to the intermediate routers and is incompatible with Internet-scale measurements. Given that hybrid measurements use passive and active techniques, they suffer from the same problems as passive and active measurements [35].

D. *Active vs. Passive Measurements*

Passive measurements are best used when the capture locations can be freely chosen, allowing communication to be captured between sender and receiver. Active measurements must be used when choosing capture points is not possible. Active measurements may be made across a network path that the measurer cannot control. Passive procedures are frequently more precise for gauging accuracy. For example, monitoring router buffers along the network path would pinpoint packet loss. Furthermore, routers can monitor connections used to calculate available bandwidth. Both of the aforementioned metrics need active probing to be performed successfully. Table 1 compares passive versus active measurements.

The techniques and problems for these metrics can be illustrated in Fig. 6. Active techniques are primarily classified into two broad categories: file transfer/batch data transfer techniques and packet-pair techniques. This separation is made based on the technology used to create traffic and then analyze it to determine QoS metrics. Active issues are assessed, and their effects on the findings are measured, offering a broad overview of various factors to consider while actively measuring. A thorough investigation has revealed the issues affecting the findings of active measuring, including things like CPU and memory use, self-initiated traffic, ICs, and techniques for ensuring the quality of service.

Passive monitoring methods and systems are developed with a particular emphasis on three distinct approaches: flow-level monitoring, packet-level monitoring, and MRTG monitoring. Problems associated with passive measurement involve being familiar with the issues inherent in existing implementations and methods for checking the accuracy of traces and the limits of passive measuring devices, such as timestamps, packet loss, and Internet routing. Network resources are required for two measurements. Active network monitoring sends test traffic. It uses this traffic to locate bottlenecks and assess network performance. Thus, it demands additional network resources. Passive network monitoring captures, stores, and analyzes network user data to detect use patterns. It does not need any more data in the network. Decreased networking hardware overhead is caused by reduced network resource use.

TABLE I
ACTIVE VS. PASSIVE MEASUREMENTS

No.	Differences Type	Active	Passive
1	Network Resources Required	It monitors network performance and identifies bottlenecks, So it uses more network resources.	It does not need any more data in the network.
2	Analysis of Data	Active monitoring collects data on certain network characteristics to examine its performance.	It gives you a detailed picture of your network's performance. It involves examining past network traffic.
3	Amount of Data Collected	Active monitoring targets specific issues. To remedy the problem, data is produced and kept.	Passive monitoring uses previous data. It creates and saves a lot of data. The extra information helps resolve future concerns.
4	Applications	Active network monitoring assures smooth operation. Enterprises utilize active monitoring to maintain optimal network performance.	Passive monitoring is used to determine which network parts are using the most bandwidth.

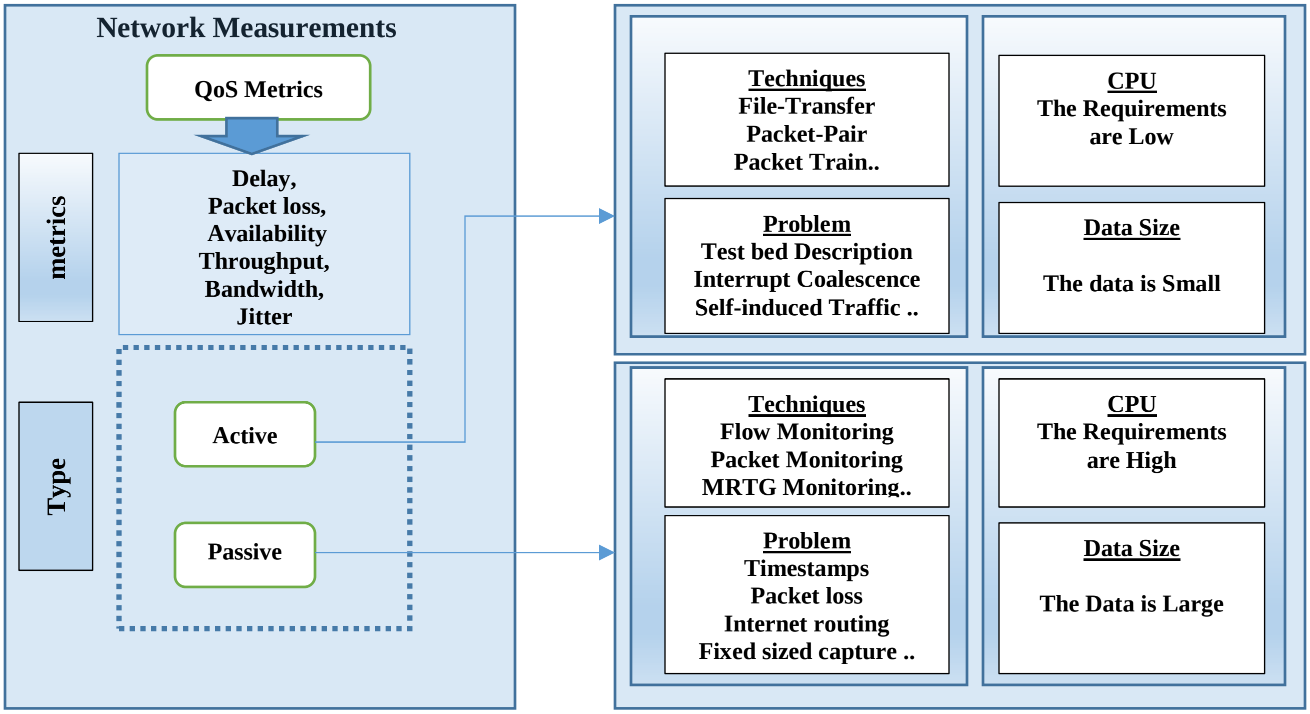

Fig. 6: The simple structure of network monitoring measurements.

E. Directions for Future Research

This evaluation covers all metrics in depth. In measuring passive advantage, a surveyor requires only a sensor and a data recorder to record a naturally existing field. Passive studies can be performed across larger areas and at a lower cost than active measures. Network operators can deduce the underlying control algorithms and analyze traffic flows. Passive measurement examines recorded packet traces to determine network flows. In contrast to active measurement, passive measurement does not introduce false traffic into the network. It merely monitors the network without generating or altering any real traffic on it. Network operators and academics in the networking world are increasingly relying on passive monitoring measurements [39], [40].

Passive monitoring measurement improves noise reduction by controlling the injected signal. The active operation takes more time and effort than a passive experiment. Furthermore, various source-receiver arrangements allow for diverse survey designs. Increasing the number of field alternatives would increase review design expenses and the likelihood of field errors. Besides, the sheer volume of data generated by several current trials[40-44]. As shown in Fig. 7, the number of publications on Network Monitoring Measurements for QoS has gradually increased since early 2011. The article count plainly shows that passive measurement is the most popular. While active measurement is a promising review field, hybrid measurement is also gaining interest.

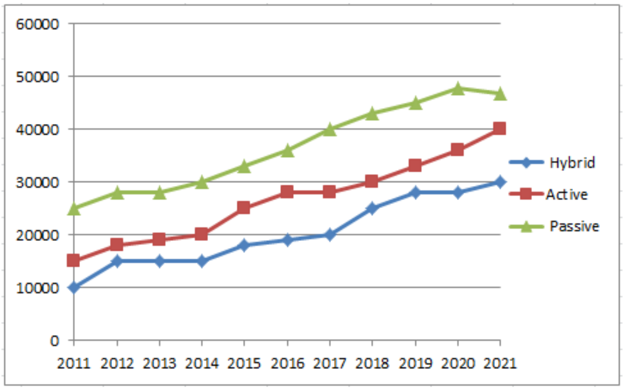

Fig. 7: Number of papers written on network monitoring measurements for QoS in measurements selection, from google scholar.

V. Wireless Network Monitoring

The preceding subjects have generally dealt with wired networks or networks in general. However, as mobility becomes the fundamental concern of Internet growth, wireless networks need particular scrutiny owing to their inherent difficulties and security dangers [12], [45], [46].

Wireless networks need a completely new set of tools for network managers because existing solutions will prove insufficient in specific ways. No cables for sniffing and reading packets and no physically continuous block of hosts for examination or isolation are available. Moreover, security becomes a major concern; whereas encryption is easier to achieve on wired networks because of their high bandwidth capabilities. Wireless networks must contend with lower data rates, forcing them to choose between security and efficiency, given that attackers are far more capable of intercepting packets. As a result, wireless network monitoring is required to ascertain if any rogue hosts or access points are trying to create a presence on or near the corporate network. Furthermore, whether users are arranging themselves appropriately can be determined; although wireless networking allows for greater geographical dispersion of systems, outlying users may only get a weak signal, resulting in performance concerns [3], [45], [46].

While wireless network monitoring requires the development of new technologies, it combines many of the same monitoring reasons, as discussed in earlier sections. Packet sniffing still gives valuable insight into user behavior and maybe more useful on wireless networks. If the administrator can quickly sniff and decode passwords and other information transferred over the network, an attacker can and will do the same. Monitoring user application activity is also crucial given that active wireless users are more exposed to attack than wired users protected by firewalls and network address translation, and finding vulnerable apps on wireless workstations is crucial. Wireless networking security concerns drive its goals and significantly impact its analyses [46], [47]. The present study shows some of the wireless network performance analysis tools that are freely accessible on the Internet or commercially [48].

A. The Public Domain

1) *Nets tumbler*: It is a free tool for wireless network investigation. This tool enables an administrator to scan wireless networks for adequate coverage, identify interference, determine the orientation of an antenna, and detect illegitimate nodes and access points by active scanning, which entails sending probes every second and logging the results. However, the Net tumbler has several drawbacks. One issue is that it is only compatible with recent Windows operating systems. As a result, many people will be unable to use it. Furthermore, the net tumbler is incompatible with some wireless networking adapters. Moreover, passive scanning is not implemented. As a result, this tool is not suitable for businesses that need to ensure monitoring of all traffic in all modes but could be adequate for most customers who do not utilize unusual network cards [48].

2) *Kismet:* It is another freeware program for investigating wireless networks. This program replaces the net tumbler that runs on Linux, BSD, Mac OS X, and Windows 32 systems. Kismet is a highly functional tool that allows for logging common data and Wireshark/tcpdump-compatible formats while also interpreting the data to produce graphical representations of network topology and comprehensive identification of access points and clients. Kismet’s capabilities enable it to be used for network analysis and intrusion detection. However, the setup time of this program is long, which

reduces the simplicity of its use even with all the capabilities enabled. Additional utilities must be downloaded to ensure proper functioning, and appropriate software adjustments must also be made. As with the net tumbler, some wireless cards are incompatible. Despite its complexity, Kismet appears to be the best free wireless network monitoring tool in capability and versatility [49].

B.The Commercial Tools:

1) *CommView*: It is software for monitoring wireless networks. CommView monitors all wireless communication and outputs complete statistics to a terminal. This data can be sorted, filtered, and examined more easily through a simple, easy-to-use user interface. Furthermore, CommView is meant to notify and warn defined people dynamically of the occurrence of specified unusual or suspicious behavior. TamoSoft praises CommView's ability to decode WEP and WPA communications. Given that WEP is rapidly losing popularity as a result of its susceptibility to attack, decoding is an important capability. The 30-day free trial offered by TamoSoft enables customers to evaluate these capabilities and determine CommView's superiority over free alternatives [50].

2) *Orion Wireless Network Monitor (Orion):* It is optimized for very high-end networks, with an exceptional user interface, features, and support. While the capabilities are named similarly to those of programs, such as CommView, the functionalities are expanded, allowing for further graphical modeling and analysis. Custom accounts could be established to avoid requiring a single administrator account to be accountable for all problems, and access restrictions can be configured for users with varying degrees of power or in separate locations. However, all come at a cost. Orion requires newer Windows PCs and is substantially more expensive than other wireless network monitoring programs. The trial version is highly suggested for testing before purchasing the full Orion product [49].

VI. Conclusions

Network monitoring is a part of reaching the objective of high performance because it aids in detecting and preventing network faults. This review examines network monitoring measurements in order to get quality service to serve as a resource for future research and application. However, passive network monitoring is not limited to issue resolution; it may also be used to generate network statistics and measure network performance. In this light, passive network monitoring, is a very strong tool, as seen by the sheer volume of data published on Google Scholar. For example, passive monitoring gives you a detailed picture of your network's performance. It creates and saves a lot of data, and the extra information helps resolve future concerns. Passive procedures are frequently more accurate. For example, monitoring router buffers along the network path would pinpoint packet loss. However, the monitoring system must be precise, simple to use, and fast enough to represent network performance in real-time. Network performance is critical to achieving service quality. Factors impacting performance include available bandwidth, network congestion, latency, server performance, and the complexity of the network management protocol. In future work, a new passive network-monitoring algorithm can be proposed using the most common metrics to deal with problems e.g. evaluating actual video streams based on how well the network is serviced.

Conflict of Interest

The authors have no conflict of relevant interest to this article.

References

[1] He, Yiran, and Xinchang Zhang. "A Survey on Network Measurement for Software-Defined Networks." *2019 3rd International Conference on Electronic Information Technology and Computer Engineering (EITCE)*. IEEE, p. 1534-1540, 2019.

[2] Charles, AS Joseph, and P. Kalavathi. "QoS measurement of RPL using Cooja simulator and Wireshark network analyser." *International Journal of Computer Sciences and Engineering*, pp. 283-291, 2018.

[3] EGILMEZ, Hilmi E., et al. OpenQoS: An OpenFlow controller design for multimedia delivery with end-to-end Quality of Service over Software-Defined Networks. In: *Proceedings of the 2012 Asia Pacific signal and information processing association annual summit and conference*. IEEE, p. 1-8, 2012.

[4] I.GHAFIR, J.SVOBODA, and V. PRENOSIL, "Network Monitoring Approaches An Overview," no. August, pp. 118–123, 2015.

[5] Y. Guo, T. Lin, K. Liang, and G. Chen, "Network Quality Monitoring for Typical Power Services," in *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, pp. 1437–1441, 2019

[6] I. O. Yuskov and E. P. Stroganova, "Application of neural network model design for monitoring wireless communication networks," in *2020 Systems of Signals Generating and Processing in the Field of on Board Communications*, pp. 1–4 , 2020.

[7] L. N. Devi, G. K. Reddy, and A. N. Rao, "Live Demonstration on Smart Water Quality Monitoring System Using Wireless Sensor Networks," in *2018 IEEE SENSORS*, pp. 1–4, 2018.

[8] H. AL-Behadili, "NTT: Network Topology Tool for Enhancing NS-2," *Iraqi J. Electr. Electron. Eng.*, vol. 11, no. 1, pp. 101–104, 2015.

[9] A. M. M. Habbal, S. Hassan, A. M. Jabbar, "JDNA: JAVABASED NS-2 ANALYZER". Wulfenia J, vol. 19, no. 9, pp. 454–462, 2012.

[10] K. M. Kim *et al.*, "Performance evaluation of maritime VDES networks with OPNET simulator," in *2018 11th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP)*, pp. 1–6 , 2018.

[11] J. Ramprasath and V. Seethalakshmi, "Improved Network Monitoring Using Software-Defined Networking for DDoS Detection and Mitigation

Evaluation,” *Wirel. Pers. Commun.*, vol. 116, no. 3, pp. 2743–2757, 2021.

[12] R. Singh and S. Kumar, “A comparative study of various wireless network monitoring tools,” in *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, pp. 379–384, 2018.

[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.

[14] Y. Sumiya and S. Maeda, “Rate constant matrix contraction method for systematic analysis of reaction path networks,” *Chem. Lett.*, vol. 49, no. 5, pp. 553–564, 2020.

[15] Mirtchev, Seferin T. "Packet-level link capacity evaluation for IP networks." *Cybernetics and Information Technologies*, pp. 30-40, 2018.

[16] S. Anand and M. V Ramesh, “Performance Analysis of Delay Tolerant Network Routing Protocols in a Heterogeneous Vehicular Network,” in *2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, pp. 1–6, 2018.

[17] T. J. Wong and N. Das, “Modelling and analysis of IEC 61850 for end-to-end delay characteristics with various packet sizes in modern power substation systems,” in *5th Brunei International Conference on Engineering and Technology (BICET 2014)*, pp. 1–6, 2014.

[18] Qu, Ting, et al. "SQR: In-network packet loss recovery from link failures for highly reliable datacenter networks." *2019 IEEE 27th International Conference on Network Protocols (ICNP)*, pp. 1–12, 2019.

[19] Moudi, Mehrnaz, and Mohamed Othman. "On the relation between network throughput and delay curves." *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, pp. 415-424, 2020.

[20] Ha, Phuong, and Lisong Xu. "Available bandwidth estimation in public clouds." *IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 238-243, 2018.

[21] A. Hosseini, M. Dolati, and M. Ghaderi, “Bulk transfer scheduling with deadline in best-effort sd-wans,” in *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pp. 313–321, 2021.

[22] B. Zhang *et al.*, “Goodput-aware traffic splitting scheme with non-ideal backhaul for 5G-LTE multi-connectivity,” in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, 2019.

[23] H. Z. Jahromi, D. T. Delaney, and A. Hines, “Quantifying the Influence of Browser, OS and Network Delay on Time Instant Metric Measurements for a Web Mapping Application,” in *2019 IEEE 19th International Conference on Communication Technology (ICCT)*, pp. 1580–1584, 2019.

[24] S. A. Rizzo, G. Susinni, and F. Iannuzzo, “Intrusiveness of power device condition monitoring methods: Introducing figures of merit for condition monitoring,” *IEEE Ind. Electron. Mag.*, vol. 7, 2021.

[25] M. Sivaram, V. Porkodi, A. S. Mohammed, V. Manikandan, and N. Yuvaraj, “Retransmission DBTMA protocol with fast retransmission strategy to improve the performance of MANETs,” *IEEE Access*, vol. 7, pp. 85098–85109, 2019.

[26] E. Max-Onakpoya *et al.*, “Augmenting cloud connectivity with opportunistic networks for rural remote patient monitoring,” in *2020 International Conference on Computing, Networking and Communications (ICNC)*, pp. 920–926, 2020.

[27] M. J. Rahimi, S. Parveen, M. Morshed, M. R. Khan, and P. Sarker, “Development of the smart QoS monitors to enhance the performance of the NS2 Network Simulator,” in *2010 13th International Conference on Computer and Information Technology (ICCIT)*, pp. 137–141, 2010.

[28] Osman, Radwa Ahmed, et al. "Quality of service optimisation of device-to-device communications underlaying cellular networks." *IET Communications*, pp. 179-190, 2021.

[29] S. Giordano, S. Salsano, S. Van den Berghe, G. Ventre, and D. Giannakopoulos, “Advanced QoS provisioning in IP networks: The European premium IP projects,” *IEEE Commun. Mag.*, vol. 41, no. 1, pp. 30–36, 2003.

[30] N. Kniazieva, S. Kotlyk, and A. Kalchenko, “Method of Assessment and Improvement the Quality of Multimedia Services,” in *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, pp. 426–430, 2019.

[31] Moravejosharieh, Amirhossein, Kourosh Ahmadi, and Saghir Ahmad. "A fuzzy logic approach to increase quality of service in software defined networking." *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)* IEEE, pp. 68-73, 2018.

[32] Hu, ZhiGuo, et al. "Evaluating QoE in VoIP networks with QoS mapping and machine learning algorithms." *Neurocomputing* 386., pp. 63-83, 2020.

[33] B. A. Setiono, “The Effect of Marketing Mix, Quality of Service and Orientation of Entrepreneurship to Competitive Advantages The People’s Market in Surabaya City,” *J. Indones. Sci. Econ. Res.*, vol. 1, no. 1, pp. 22–25, 2019.

[34] N. Gorla, T. M. Somers, and B. Wong, “Organizational impact of system quality, information quality, and service quality,” *J. Strateg. Inf. Syst.*, vol. 19, no. 3, pp. 207–228, 2010.

[35] Kaafar, Mohamed Ali, Steve Uhlig, and Johanna Amann, ”*Passive and Active Measurement*”, Springer International Publishing, pp. 30–31, 2017.

[36] B. Widera, P. Dost, V. Kipke, and C. Sourkounis, “On optimal cell monitoring in a sensor minimal battery management system with integrated direct active balancing,” in *2019 IEEE Industry Applications Society Annual Meeting*, pp. 1–8 , 2019.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] Kumar, Rajeev. "Passive Bandwidth Estimation Techniques for QoS Routing in Wireless LANs." *Soft Computing for Problem Solving*. Springer, Singapore, p. 443-452, 2020.

[42] F. P. Garcia, R. Andrade, C. T. Oliveira, and J. N. De Souza, "EPMOSt: An energy-efficient passive monitoring system for wireless sensor networks," *Sensors*, vol. 14, no. 6, pp. 10804–10828, 2014.

[43] R. Zheng, T. Le, and Z. Han, "Approximate online learning for passive monitoring of multi-channel wireless networks," in *2013 Proceedings IEEE INFOCOM*, pp. 3111–3119, 2013.

[44] E. Browning, R. Gibb, P. Glover-Kapfer, and K. E. Jones, "Passive acoustic monitoring in ecology and conservation.," 2017.

[45] J. T. Wen and Y. Geng, "Environment monitoring system of household security robot based on wireless mesh network," in *2009 International Conference on Networks Security, Wireless Communications and Trusted Computing*, vol. 2, pp. 176–180, 2009.

[46] M. Hu and Y. Wang, "Design of Wearable Wireless Body Area Network Monitoring System," in *2020 IEEE 3rd International Conference on Information Systems and Computer Aided Education (ICISCAE)*, pp. 585–588, 2020.

[47] C. C. Ho, K. N. Ramachandran, K. C. Almeroth, and E. M. Belding-Royer, "A scalable framework for wireless network monitoring," in *Proceedings of the 2nd ACM international workshop on Wireless mobile applications and services on WLAN hotspots*, pp. 93–101, 2004.

[48] S. Rahane, S. Ulekar, R. Vatti, T. Meshram, and S. Male, "Comparison of wireless network performance analysis tools," in *2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)*, 2018, pp. 1–4.

[49] A. D. Ferguson *et al.*, "Orion: Google's {Software-Defined} Networking Control Plane," in *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*, pp. 83–98 2021.

[50] R. Arunadevi, "Experimentation Of Denial Of Service Attack In Wireless Local Area Infrastructure Network Using Loic Tool," *J. Eng. Res. Appl.*, pp. 51–55, 2018.