QoS Performance Metrics for Analyzing Wireless Network Usability

OMOMULE T. G.[1], OLARINDE D. O.[2], UGWU C. C.[3], FALANA T. A.[4]
[1, 2] *Department of Computer Science, AdekunleAjasin University, Akungba-Akoko, Ondo State, NIGERIA*
[3, 4] *Department of Computer Science, the Federal University of Technology, Akure, NIGERIA*

Abstract- ***The increasing rate of Internet users has caused the storage of tremendous amount of data and the rise in web traffic resulting to network congestion, web service delay and slow response time. These network bottlenecks have affected the services and performance experienced by the users thereby posing a serious question against the network reliability and usability. This paper analyzes the usability of a wireless network and its performance based on the quality of service (QoS) experienced by the network users. A huge amount of distinct packets were collected on 1,476 installed access points using wireshark packet tool over a period of three weeks for data pre-capturing at experimental stage. Experimental analysis was carried out using a number of QoS parameters subject to the network resource requirements and usability. Experimental results showed the usability indices for each QoS parameter and the practicality of traffic patterns, user behaviours and other QoS parameters in measuring network usability.***

Indexed Terms- ***Performance Metrics, Packets, Quality of Service (QoS), Usability, Wireless Network.***

I. INTRODUCTION

Over the years, the use of computer networks has provided huge benefits to mankind via the Internet in several domains such as education, business, banking and defense (Arun, 2018). These interconnected set of computer system permits interactive resource sharing between connected pair of systems either wired or wirelessly (Wierenga and Florio, 2005). However wireless communications are becoming widespread in many fields and commonplace in many environments, and people are also adapting to the on-the-go connection of computer networks (Tang and Baker, 2002). Users are increasingly interested in taking advantage of the flexibility of wireless technology, and a boom in its implementation to local area networks has also been experienced (Blinn*et al.*, 2005). Universities have pioneered the development of infrastructures to provide connectivity such as the Wireless Andrew at the Carnegie Mellon University campus; an enterprise-wide broadband wireless network developed in 1993. This motivated several study of wireless networks on campus-wide scenarios to understand the level of usage for efficient allocation of network resources to meet the time and cost requirements of institution's management objectives. This level of network usage largely depends on the way in which data are collected; *tcpdump*, the Simple Network Management Protocol (SNMP) and *syslog* are the most common tools. *Tcpdump*is normally used to sniff the traffic and analyze the applications run by users and the amount of data managed in the network while a SNMP (Simple Network Management Protocol) tool is applied to periodically poll the access points (APs) of the network and to obtain information regarding the authenticated associated users and their approximate location, that is, the coverage range of the AP to which a user is associated). Information on the authenticated or associated devices at each AP can also be obtained through *syslog*, a standard for forwarding log messages in an IP (Internet Protocol) network, although polling-based trace collection is suitable for usage statistics, it is not very suitable for deriving the association patterns of users because details of association changes are overlooked due to the polling interval. Differences may also be found in the duration of the period analyzed; some span a period of a week, in which case weekly cycles cannot be observed, others one month, and others three to five months. (Tang and Baker, 2002).

The increasing rate of Internet users has caused the storage of tremendous amount of data and the rise in

web traffic resulting to network congestion, web service delay and slow response time. These network bottlenecks have affected the services and performance experienced by the users thereby posing a serious question against the network reliability and usability. This paper analyzes the usability of a wireless network and its performance based on the quality of service experienced by the network users.

Usability lies in the interaction of the user with the product or system and can only be accurately measured by assessing users' performance, satisfaction and acceptability. Any change in the characteristics of the product or system, user, task or environment may produce a change in usability. Quality of Service (QoS) measures the level of performance of particular routing protocol of service providing to network end users.

II. RELATED WORKS

The diversified development of information technology has not only increased demand for Internet access, but also brought heavier network traffic loads. As revealed in Adya*et al.,* (2002), the greatly increased user demands have caused the Internet to successfully evolve into a mainstream market from an esoteric niche and at the same time brings about challenges in the usability of the network. In a bid to investigate the performance analysis of a network especially in the education domain, several authors have used different approaches to get varying results based on different type of techniques, metrics and parameters. Kotz and Essien (2002) presented an analysis of a campus wide wireless network to study and carry out a network scalability of an institution. Three data collection techniques, syslog events, SNMP polling, and tcpdump sniffers were used to collect data about wireless network usage which include: The traffic workload is quite extensive both in scope as about 1706 users across 476 access points were recorded and a total time duration of 12weeks. The trace collection is a reflection of the large-scale characteristics of the campus WIFI, which includes its overall application mix, overall traffic per building, AP and mobility patterns. A much larger fraction of the traffic was found to be addressed to an unknown ports, and traffic from backup applications. The mobility patterns were analyzed with respect to the size of their network but usability information were not collected about network. Also power outage during the tracing period created spatial and temporal holes in the usability trace analysis.

Balachandran *et al.,* (2002) characterized users' behavior and network performance in a public wireless LAN using a parameterized model. The analysis of a trace recorded over three days was done. The trace consists of two parts. The first part is a record of performance monitoring data sampled from wireless access points (APs) serving the conference and the second consists of anonymous packet headers of all wireless traffic. Both parts of the trace span the three days of the conference, capturing the workload of 300,000 flows from 195 users consuming 4.6 GB of bandwidth. The research applied the workload analysis to better understand issues in wireless network deployment such as capacity planning, and potential network optimizations. The work failed to capture a realistic characterization of mobile users' network activity.

Soft computing techniques were applied to analyse the performance of a wired and wireless LAN in Bansal *et al.,* (2010). The objective was to simulate the performance between wired and wireless network based on some specific performance metrics such as throughput, delay, and retransmission attempt. OPNET protocol analyzer was used to perform a soft computing simulation in a stochastic and deterministic environment. The author failed to analyze the network usability in the simulated environment.

Mistry *et al.,* (2016) worked on network traffic measurement and analysis. Different network monitoring tools and approaches were used to monitor and analyze network traffic using different protocol tools such as wireshark, Ntop, microsoft message analyzer and PRTG. An intimate comparison between the passive monitoring protocol tools based on their mode of operation and analytic graphic interface design was carried out. The authors emphasized on the minimization of packet loss as well as the capability to handle large traffic data but experienced insufficient volume of traffic and logs from communicating nodes over the network which

could be used to characterize the packet captured for each protocol tools.

Blinn*et al.,* (2015) analyzeWiFi hotspot network using parameters such as number of users, number of access points (APs) and traffic statistics. Network activity trace lasting approximately for five weeks from the Verizon WiFi Hotspots network using the Simple Network Management Protocol (SNMP) tool were collected. The SNMP tool was used to poll the Verizon Wi-Fi Hotspot network every 5minutes from a variety of access point's available running the IEEE 802.11b. Polls collected information on users including MAC address, AAA State, bytes sent and received. Once received, messages were time-stamped using the pooler's clock. The result is significant in characterizing the access point traffic distribution over time and assessing the spatial correlation existing among adjacent access points. However, crashes and breakdown in the data collection process limit effective usability analysis of the network.

Chuvak and Surovtsova (2018) discussed the analysis of user activity in wireless local area network of Petrozavodsk State University. They performed an experiment to measure the activity of users in a wireless networks environment and also to collect data on wireless network users and apply the information obtained for calculation of allowed rate constrains. The authors developed a method to determine users' activity without access to the service equipment and personal data, as well as a software complex to implement this method. A Python application that features a dynamic type system and automatic memory management based on utility Nmap for network scanning using ARP-queries and automates computer switching between networks was developed to monitor and collect data from several network operations simultaneously. Data collected were analyzed on the hours of the highest and lowliest activity, class schedule effect, and the dynamics of users' returns to the network. The information obtained determined the allowed constraints of the Internet access speed for network users without considering relevant constraints of data collected from users. A wireless LAN design framework for optimal placements of access points at suitable locations to satisfy the coverage and capacity requirements of the users is introduced by Chandrashekhar and Janes (2009). Optimal planning of WLANs can help improve Quality of Services, efficient use of resources, minimize interference and reduce deployment cost. Randomized optimization algorithm was used to solve the AP placement and channel allocation problems like coverage, traffic, Redundancy, channel interference and wiring cost. The implementation was carried out using OPNET. The authors established IEEE 802.11 theoretical throughput limit depending on the network configuration but the work was affected by a bandwidth limitation in the WLAN due to the error prone physical medium.

Divgi and Chlebus (2007) characterized users' activity and traffic in a commercial nationwide WiFi hotspot network based on their account time limits and the impact of account stratification on the overall user behavior. The research was based on the examination of user activity log and traffic volume collected by a wireless network service provider operating hotspots. A similarity index model was used to compare two datasets of unknown distributions which was then used to quantitatively compare how similar or different various types of accounts are. The user population of the network is found to be highly fluctuating, hence metrics to measure account time and data utilization of user specification, population independent were proposed to account for this transience. Therelationship of similarity of user accounts usingusage metrics is quantified but the applicability of the similarity index model used for the network usage analysis was not merged with the individual and global metrics. Soldo and Malarić (2013) presents the measurements of WiFi signal strength in a WLAN. The authors examined how signals were measured and analyzed using tablet. The device used was saturated with a couple of applications and a built-in Wi-Fi antenna. Several measurements were conducted repeatedly to show the influence of different factors on the strength of the Wi-Fi signal and on the download and upload speed. The authors opted for the Google Nexus 7 tablet for measurements since it supports Wi-Fi 802.11 b/g/n as well as Bluetooth and also operates on 4.2 Android operating system. Two Android applications were installed on the measuring device used, the first being a"Wi-Fi Analyzer" to select a

better channel to scannearby wireless access points and shows spots with best signal strength and least traffic and the other been an application "Speedtest.net" which was used to measure the networkdownload and upload speed. The results showed an increased measurement rate of Wi-Fi signal but cases of network interference affects the experimentation download and upload link.

In the work of Sulaiman and Yaakub(2010), the investigation of QoS on Campus-wide WiFi Networks in term of performance analysis and connectivity problems affecting WiFi usability is carried out. To simulate the network usability behaviour, different brand of laptops including clone computers and several types of passive tools were used such as Fluke Network Inspector, Network Stumbler, WildpacketsAiroPeek NX, WildpacketsiNetTools, WiFi Manager, Commview for WiFi and LviewPro. A study on the WiFi coverage was also carried out by auditing both the wired and the wireless networks, as well as the saturation level of the Access Point. The work combined and analyzed the factors that cause wireless network problems but failed to properly address channel overlapping and saturation conditions occurring at the latter stage of the experimentation.

III. NETWORK QOS PARAMETERS

Quality of Service (QoS) is a concept whereby computing and network resources works in line with the users' and operational objectives. It ensures performance guarantee in relation to computing cost and time, availability and reliability of using computing resources. Computer network performance may vary due to quality of service guarantees, such as the problem of packet loss, delay (latency), jitter and throughput etc, which can lead to inconsistent performance of many applications. This is presented in Figure 1 as follows:

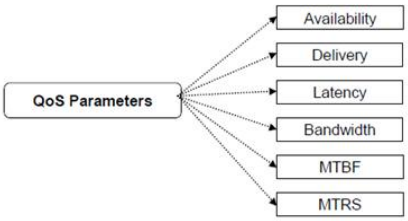


Figure 1: QoS Parameters for Network QoS (Lee, 2003)

3.1 The Study Environment

The experimentation of this research was carried out in the main campus of AdekunleAjasin University, AkungbaAkoko, (AAUA) Ondo State, Nigeria, a public university, owned and managed by the state government. To analyze AAUA wireless network, the knowledge of its geographic and demographic composition is captured. This information provides preliminary insight into the users' community. The school campus is compact, with over 161 buildings, including administrative, academic, residential, and athletic buildings. Every building is wired to the campus backbone network. Every office, dormitory, and lecture hall, has wired Ethernet. The school has over 1476 wireless access points which comprises of Aironet model, T-P Link model and D-Link model among others, which are used to provide transmission to nearly the entire campus. Each access point (AP) has a range of about 130–350 feet indoors, so there are several APs in all but the smallest buildings. Although there was no specific effort to cover outdoor spaces, the campus is compact and the interior APs tend to cover most outdoor spaces. All APs share different network name (SSID), limiting wireless clients to roam seamlessly from one AP to another. On the other hand, a building's APs are connected through a multi-layer switch or hub to the buildings' existing subnet. The 100 covered buildings span 81 subnets, so in many cases a wireless client roaming from one building to another will be forced to obtain a new IP address dynamically with a configured DHCP enabled router. AAUA has about 11,500 students and has over 1,215 full-time lecturers. Statistics shows that approximately 3,330 undergraduate students on campus own a computer. The WLAN topology of AAUA is presented in Figure 2 while Figure 3 shows a sample of the wireless access points in AAUA as follows:

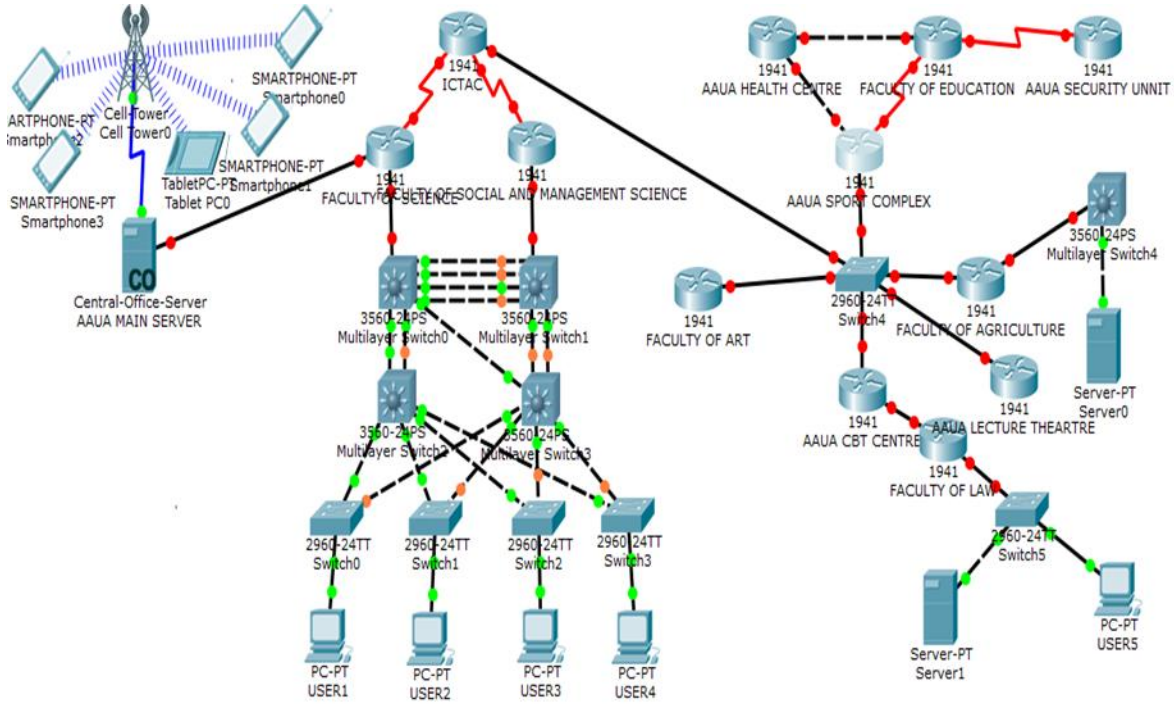


Figure 2: AAUA Wireless LAN topology

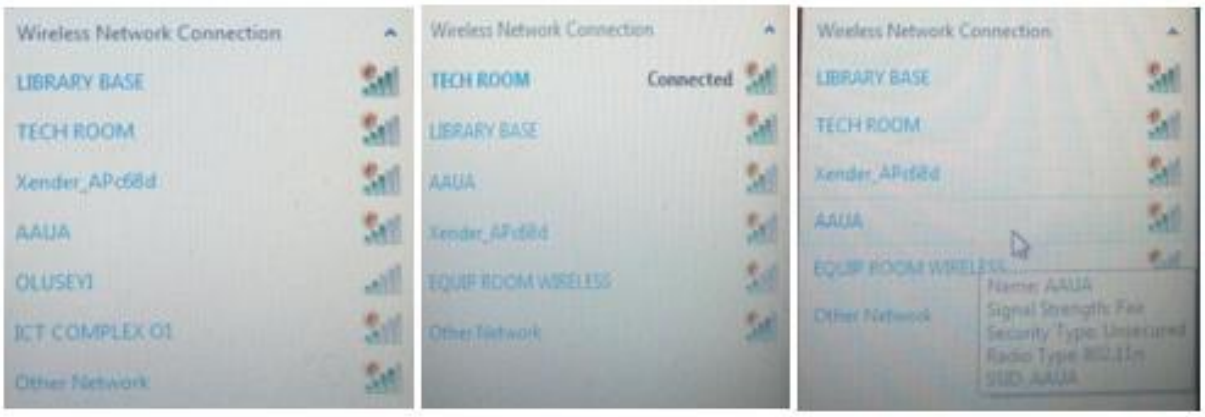


Figure 3: AAUA wireless access point deployed on campus

IV. EXPERIMENTAL ANALYSIS

This section describes the experimental stages for the usability analysis of AAUA WLAN based on QoS Performance Metrics. The packets capture and simulation were experimented using network analyzer tool where network packet or data were captured from AAUA WLAN and experimented from using Wireshark software version 3.7.

4.1 Experimental Requirements

The experimental requirements are categorized into two main parts, software and hardware requirements. The network packet data capture forms a major component for the usability analysis.

a. Software Requirements
   i. Wireshark version 3.7
   ii. liveAmchart.com
b. Hardware Requirements
   i. PC, 2.6 GHz Processor, 4GB RAM, 500GB HD
   ii. Network Interface Card (NIC)

iii. Router
iv. Cat cable 6e

c. Packet Data Requirements
i. Pcapng file of AAUA WLAN

4.2 QoS Metrics

The network analysis parameters used are outlined below but analyze in detail on section 5.

i Network Throughput.
ii Network Bandwidth.
iii Network Latency / End-to-end Delay.
iv Network Jitters.
v Network Packet loss.
vi Network Loss Rate.

4.3 Packet Data Description

The packet data used in the analysis of the QoS parameters was sourced from wireless users connected to the AAUA WLAN. An enormous number of packets data was collected and represented by only a subset of the interesting characteristics based on the QoS parameters. However, it is pertinent to note that all packet data has different structure for all parameters except in their respective protocol. The wireless network data used is provided as a supplementary data capture file (.pcapng) formats that was merged for five working days over the course of three weeks packets data captures:

a. week1.pcapng,
b. week2.pcapng,
b. week3.pcapng.

Each row in the packet file describes the number of a specific packet captured when users are connected to the wireless network. The packet data file is named as "week1.pcapng, week2.pcapng, and week3.pcapng" all merged as "aaua_wireless_data_packet.pcapng" where the length of each serial number is the number of packets in the file that has the sizes of 894,510 packets with load time of 0:23.504 seconds. The .pcapng file consists of a set of rows, where each row has a numeric value presenting the size and attributes of a given or highlighted packets. The first stage of experiment of the network analysis is data pre-capturing that was donebywireshark network analyzer tool environment while the main parameters were carried out using liveAmchart.com. File follows a long-tailed distribution (with 90% of the packets completing on average within some hours when the wireless network was still on for the day).

V. EXPERIMENTAL RESULTS AND ANALYSIS

This section presents the experimental results derived in the research

5.1 Packets Data Collection Trace

In the 15-days of the three-week trace periods after the packet collected was merged using Wireshark Network Analyzer software, 894,510 distinct packets with load time of 0:23.504. The 1,476 installed access points distribution was given by 430 by syslog, 557690 by TCP (62.3%), 3319 by HTTP (0.4%), 12464 by DNS (1.4%), 451 by SNMP, 45430 by ARP (5%), 7435 by IGMP (0.8%), ICMP (0.1%), 57128 by LLMNR (6.4%), 39778 by SSDP (4.4%) and 527 by UDP, DHCP,NBNS. The distribution of protocol captured on life wire is presented in Figure 5:

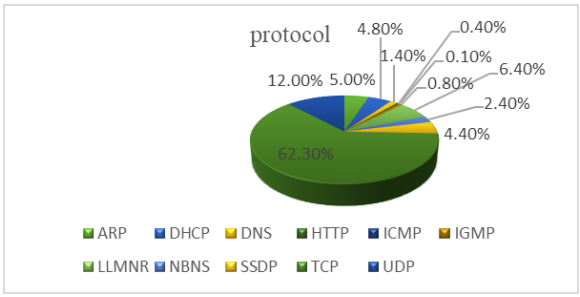


Figure 5: Distribution of Protocol captured on life Wire

The access points were distributed among 161 buildings, which was divided into the following categories: 82 Hostel Residence, 32 Academic, 20 Library, 33 Security Unit , 22 Administrative, 67 Health Centre, 26 Centre for Biology and Drug Development (CBDD), 150 Faculty of Science, 120 Faculty of Arts, 140 Faculty of Social and Management Science, 80 Faculty of Agriculture, 50 Faculty of Law, 147 Faculty of Education, 15 Career Advancement Office, 10 Centre for Space Research and Exploration, 25 CBT-Centre, 6 Centre for Gymnastics, 8 Works Unit, 20 Students Affairs Village, 10 GST-Unit etc. The distribution of

wireless access points is depicted in Figure 6 as follows:

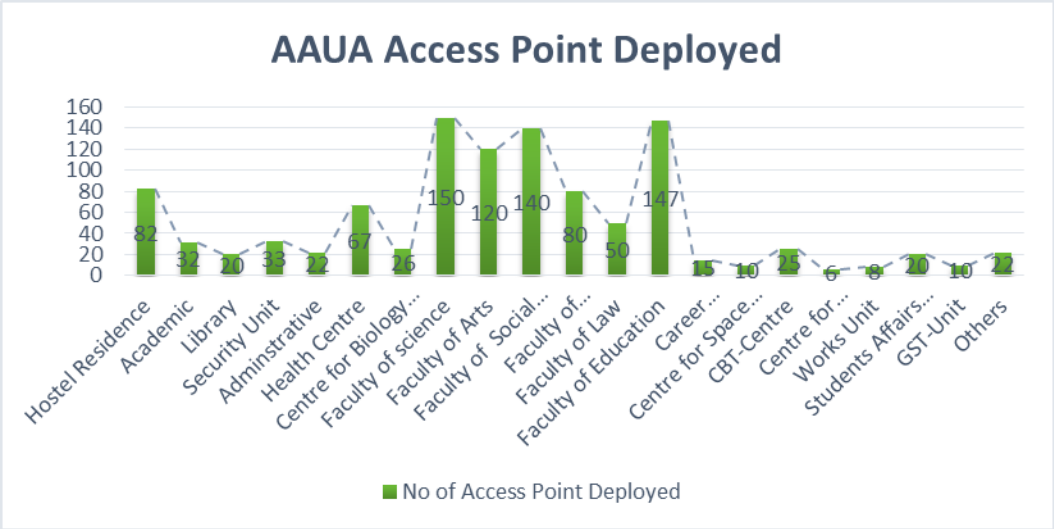


Figure 6: Wireless Access points Distribution in AAUA WLAN

The hostel residential buildings are female undergraduate dormitories, but also include some offices for staffs. All other external users have laptops and (as the data shows) while many are busy wireless users. The social buildings include Students Union Building (SUB), and athletic facilities (including a lodge at the permanent site area, OBJ-Hall and the Nelson Mandela Hall). Table 1 shows the captured packets over the course of three weeks.

Table 1: Packet data capture from AAUA WLAN for three weeks.

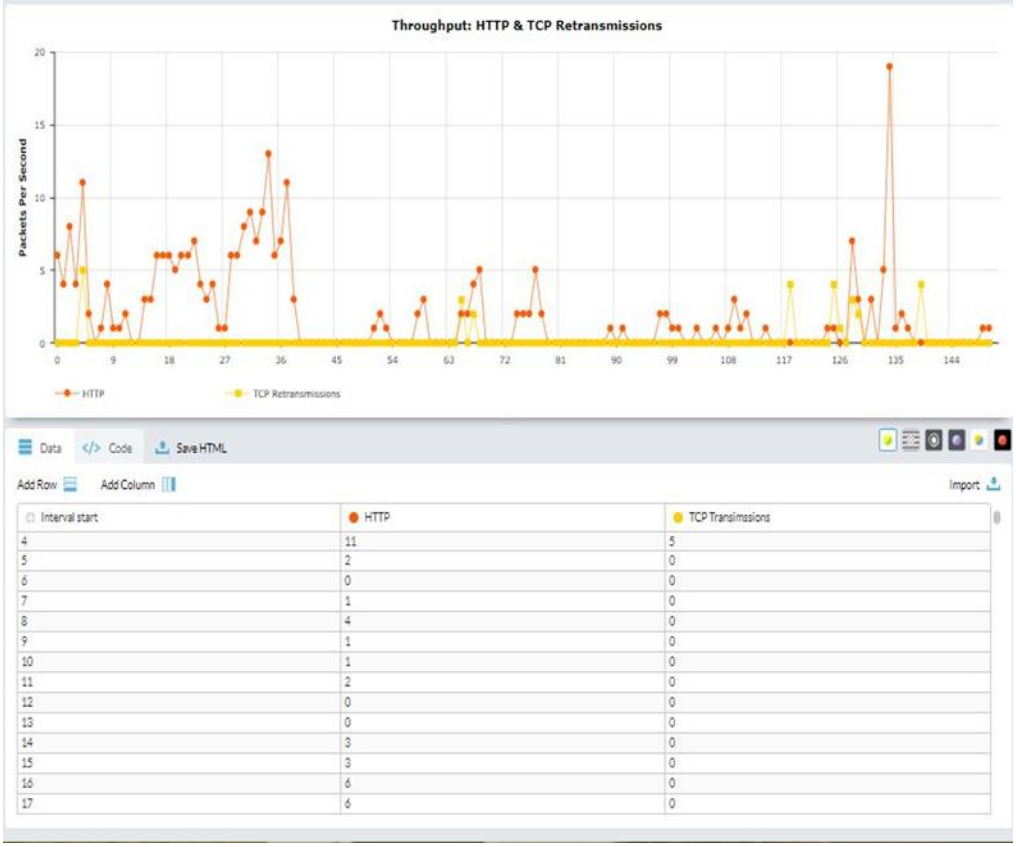
Week	Total Number of packet capture for each week
1	199,157
2	298,170
3	397,183

5.2 Network Throughput

Throughput is a measure for the amount of data transferred across a link or network at a certain time. Usually expressed in bits per second (bps), bytes per second (Bps) or packets per second (pps). The computation of network throughput is given as:

$$throughput = \frac{Total\ packet\ (bit)}{Total\ time\ delivery\ (s)} \quad (1)$$

The graph plotted in Figure 7 characterizes the behavior of data throughput as the user density increases and is given by HTTP & TCP Retransmissions with a variance of byte per seconds over the packets. This means that the network offers a data throughput of 19.7 bps when no service user has been added to the network but the network data throughput decreases by a factor of 0.1066 second for any one user added. The plot of Received bandwidth signal strength behavior is shown in Figure 7**.** Basically, in telecommunications, received signal strength index (RSSI) is a measurement of the power present in a received radio signal. RSSI is usually invisible to a user of a receiving device. However, because signal strength can vary greatly and impact on functionality in wireless scenarios, the IEEE 802.11 devices often make the measure available to users as captured with the sniffing tool used.



Interval start	HTTP	TCP Transimssions
4	11	5
5	2	0
6	0	0
7	1	0
8	4	0
9	1	0
10	1	0
11	2	0
12	0	0
13	0	0
14	3	0
15	3	0
16	6	0
17	6	0

Figure 7: Throughput Behavior for AAUA wireless Network

In general, it was found that packets throughput reaches peaks of 20(Byte/Sec) and that average throughput is caused 10(bit/s) of the time by a multiple users and application, usually a large file transfer. On average, the incoming traffic is heavier than outgoing traffic, but the periods of peak throughput are actually skewed more towards outgoing bytes. The result showed significant asymmetry in network capacity would not be desirable for wireless users. Also in the network's application mix, low per-packet processing overhead to handle many small packets is just as important as high overall attainable byte throughput.

5.3 Network Bandwidth

Bandwidth defines the transmission capacity of an electronic line. It is the degree to which the network makes an effective use of bandwidth i.e. network resources and given as:

$$Bandwidth\ Utilization = \frac{data\ volume}{duration\ priod * speed} \quad (2)$$

The network bar chart plotted in March 2019 for the three weeks characterizes the behavior of the received network bandwidth signal strength as the distance from the access points increases is given 5 + x Mb/s. This means that the received bandwidth signal strength at the access point base station is 1dB but decreases by a factor of 0.1dB for any packet's length away from the access point to the user connected to the network wirelessly. Figure 8 shows the bandwidth consumption of AAUA network users

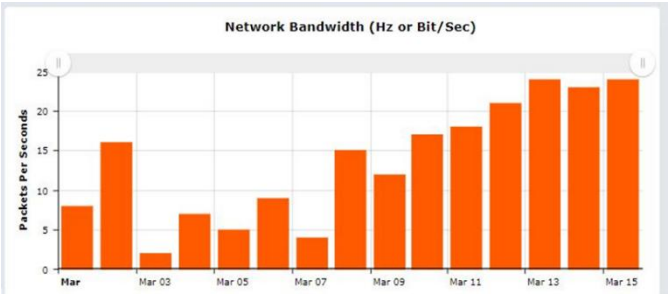


Figure 8: Bandwidth Strength Behavior for AAUA wireless Network

5.4 Network Delay or Latency

Delay is the time delay taken by a packet to travel from source to destination in a network as presented in equation 3 as follows:

$$time\ delay = \frac{Packet\ length\ (bit)}{link\ bandwidth\ (bits)} \qquad (3)$$

The plotted bar chart above characterizes the behavior of Network delay / Latency as the user density (i.e. number of user) increases in the present month of March 2019 with a variance of 5 seconds. This means that the network offers heavy delay in 11th day of March 2019 when no service user has been added to the network but the network delay to data traffic increases by a factor of 0.001 Mb/s for any one user added. Figure 9 shows the network latency behavior.

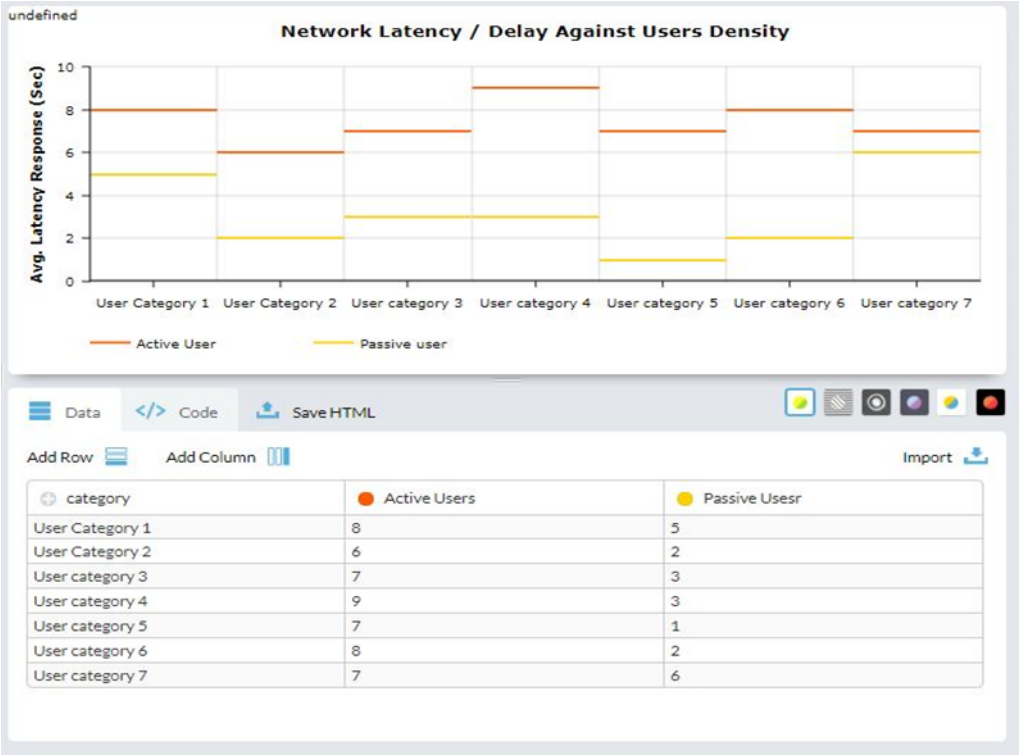


Figure 9: Delay or Latency Behavior for AAUA wireless Network

5.5 Network Jitter

Jitters is the variation in the delay of received packets as given in equation 4 as follows:

$$jitters = \frac{variation\ delay}{packet\ received} \qquad (4)$$

In the wireless network capture using Wireshark network analyzer, packet jitter variation (PJV) is the variation in latency as measured in the variability over time of the end-to-end delay across the wireless network. Monitoring the number of wireless network user, it was observed that delay has no packet jitter. Packet jitter is expressed as an average of the deviation from the network mean delay. PJV is an important quality of service factor in assessment of network performance. Transmitting a packet according to the campus wireless as number of user increases, traffic at a high rate followed by an interval or period of 20sec or 25sec rate transmission, was seen as a form of jitter, as it represents a deviation from the average transmission rate per user on the network. However, unlike the jitter caused by variation in latency, transmitting in bursts may be seen a desirable feature. Figure 10 shows the network jitter behaviours on AAUA WLAN

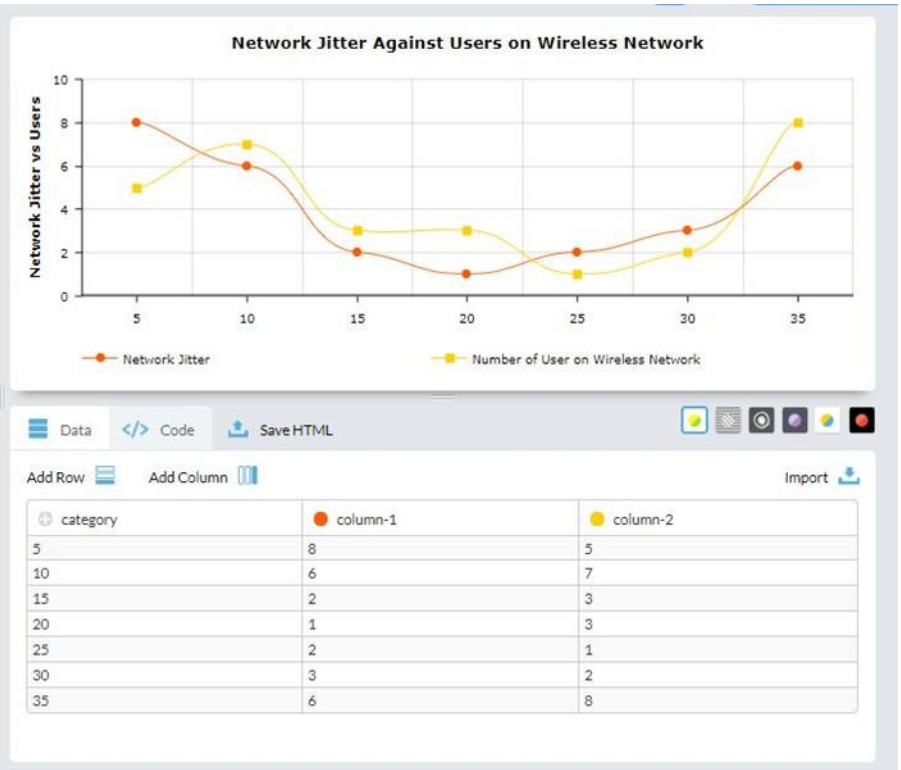


Figure 10: Network Jitter Behavior for AAUA wireless Network

5.6 Network Packet Loss and Loss Rate

Packet loss was measured as frame loss rate defined as the percentage of frames that should have been forwarded by a network but were not. The network packet loss and loss rate are computed as follows:

Network packet loss is the fraction of packets lost in transit from client to server and back during a specified while loss rate for some interval is the ratio of packets lost to the sum of packets lost and packets successfully delivered during that interval. They are computed in equations 5 and 6 as follows:

$$Packet\ loss = \frac{packets\ sent - packets\ reeived \times 100\%}{packets\ sent} \quad (5)$$

$$loss\ rate = \frac{packets\ lost}{\text{sum of packets lost}} \quad (6)$$

As shown in the figures 11, 12 and 13, packet loss is closely associated with Quality of Service (QoS) considerations, and is related to the byte/packet. The amount of packet loss that is acceptable during the analysis depends on the type of data being sent via wireless network capture. For example, IPv6 and IPv4 traffic, one indicator shows that missing one or two packets A -B and Byte A-B every address A & B will not affect the quality of the conversation. On the Figure 10 losses between 95.1% and 60.5% of the total packet stream will affect the quality significantly. Another described less than 1.7% & 8.7% packet loss as "good" for streaming data by users connected wirelessly, and 1-2.4% as "acceptable". On the wireshark interface that when multiple users transmit a text document or web page, a single dropped packet could result in loss on the part of the file, which is why a reliable delivery protocol would be used for this purpose to retransmit dropped packets as shown in figure 12. Packet loss was detected by application protocols such as TCP etc., but when Wireshark, the network analyzer tool used detects and diagnose packet loss, it typically used a purpose built-in tool, many protocols have status pages or logs, and where the number or percentage of packets dropped over a particular period was derived. For remote detection and diagnosis, the Internet Control Message Protocol provides an "echo" functionality, where a special packet is transmitted that always produces a reply after a certain number of network hops, from whichever node has just received it. Tool such as tcp analysis flag, traceroute, and MTR use this protocol

to provide a visual representation of the path packets are taking, and to measure packet loss at each user connected to the wireless network.

It was observed that packet loss reduce throughput for a given sender on the usability on wireless network, whether unintentionally due to network malfunction, vulnerability of the system, noise interference, packet congestion or intentionally as a means to balance available bandwidth between multiple senders when a given router or network link reaches nears its maximum capacity. When reliable delivery is necessary, packet loss increases latency due to additional time needed for retransmission. Assuming no retransmission, packets experiencing the worst delays might be preferentially dropped (depending on the queuing discipline used), resulting in lower latency overall at the price of data loss. During typical network congestion, not all packets in a stream are dropped. This means that un-dropped packets will arrive with low latency compared to retransmitted packets, which arrive with high latency. Not only do the retransmitted packets have to travel part of the way twice, but the sender will not realize the packet has been dropped until it either fails to receive acknowledgement of receipt in the expected order, or fails to receive acknowledgement for a long enough time that it assumes the packet has been dropped as opposed to merely delayed. Figures 11 and 12 shows the IP conversion process and protocol hierarchy of AAUA network while Figure 13 depicts the network packet loss on AAUA network.

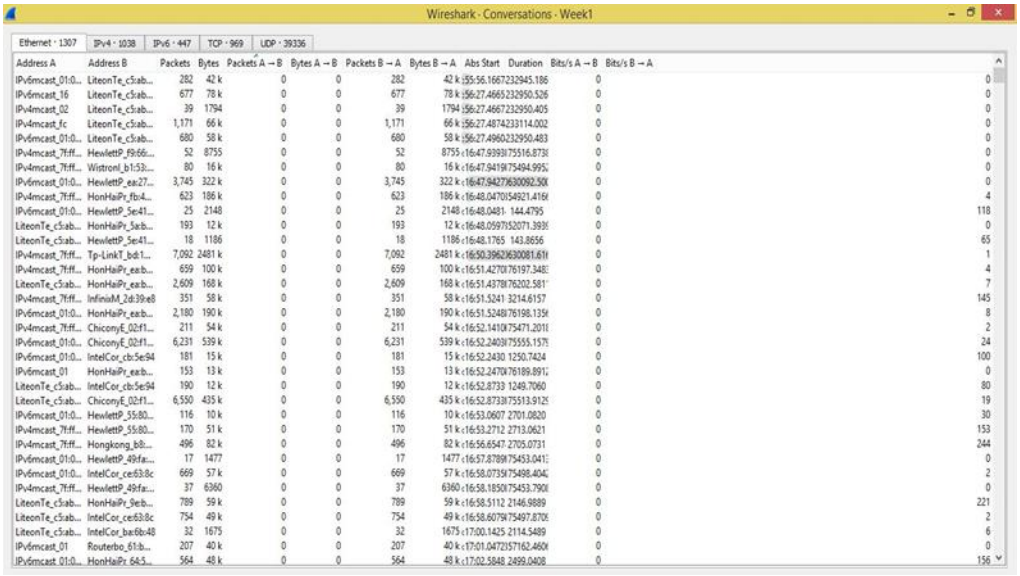
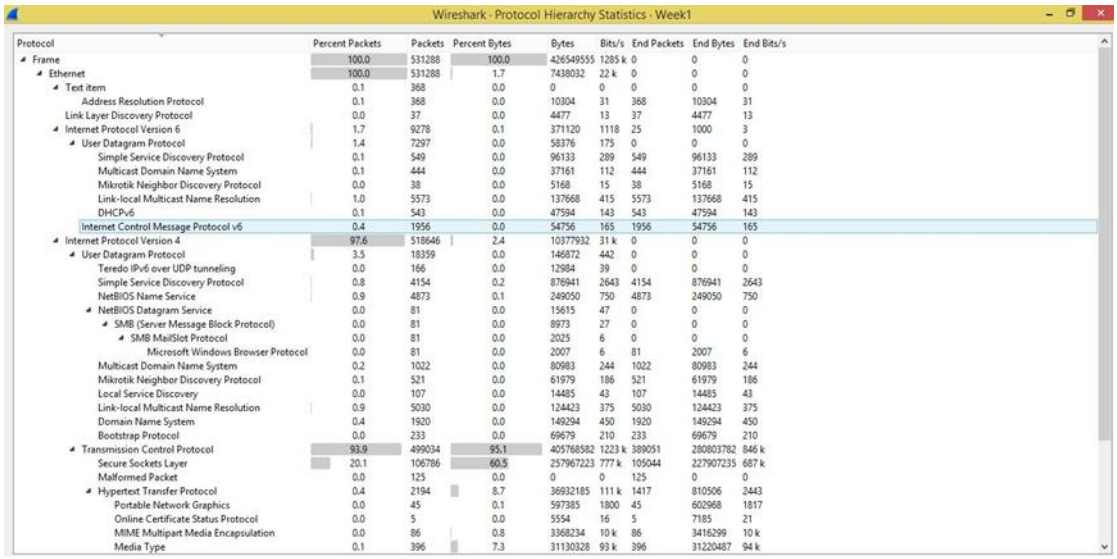


Figure 11: Conversion between IP's on AAUA wireless Network



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	531288	100.0	426549555	1285 k	0	0	0
Ethernet	100.0	531288	1.7	7438032	22 k	0	0	0
Text item	0.1	368	0.0	0	0	0	0	0
Address Resolution Protocol	0.1	368	0.0	10304	31	368	10304	31
Link Layer Discovery Protocol	0.0	37	0.0	4477	13	37	4477	13
Internet Protocol Version 6	1.7	9278	0.1	371120	1118	25	1000	3
User Datagram Protocol	1.4	7297	0.0	58376	175	0	0	0
Simple Service Discovery Protocol	0.1	549	0.0	96133	289	549	96133	289
Multicast Domain Name System	0.1	444	0.0	37161	112	444	37161	112
Mikrotik Neighbor Discovery Protocol	0.0	38	0.0	5168	15	38	5168	15
Link-local Multicast Name Resolution	1.0	5573	0.0	137668	415	5573	137668	415
DHCPv6	0.1	543	0.0	47594	143	543	47594	143
Internet Control Message Protocol v6	0.4	1956	0.0	54756	165	1956	54756	165
Internet Protocol Version 4	97.6	518646	2.4	10377932	31 k	0	0	0
User Datagram Protocol	3.5	18359	0.0	146872	442	0	0	0
Teredo IPv6 over UDP tunneling	0.0	166	0.0	12984	39	0	0	0
Simple Service Discovery Protocol	0.8	4154	0.2	876941	2643	4154	876941	2643
NetBIOS Name Service	0.9	4873	0.1	249050	750	4873	249050	750
NetBIOS Datagram Service	0.0	81	0.0	15615	47	0	0	0
SMB (Server Message Block Protocol)	0.0	81	0.0	8973	27	0	0	0
SMB MailSlot Protocol	0.0	81	0.0	2025	6	0	0	0
Microsoft Windows Browser Protocol	0.0	81	0.0	2007	6	81	2007	6
Multicast Domain Name System	0.2	1022	0.0	80983	244	1022	80983	244
Mikrotik Neighbor Discovery Protocol	0.1	521	0.0	61979	186	521	61979	186
Local Service Discovery	0.0	107	0.0	14485	43	107	14485	43
Link-local Multicast Name Resolution	0.9	5030	0.0	124423	375	5030	124423	375
Domain Name System	0.4	1920	0.0	149294	450	1920	149294	450
Bootstrap Protocol	0.0	233	0.0	69679	210	233	69679	210
Transmission Control Protocol	93.9	499034	95.1	405768582	1223 k	389051	280803782	846 k
Secure Sockets Layer	20.1	106786	60.5	257967223	777 k	105044	227907235	687 k
Malformed Packet	0.0	125	0.0	0	0	125	0	0
Hypertext Transfer Protocol	0.4	2194	8.7	36932185	111 k	1417	810506	2443
Portable Network Graphics	0.0	45	0.1	597385	1800	45	602968	1817
Online Certificate Status Protocol	0.0	5	0.0	5554	16	5	7185	21
MIME Multipart Media Encapsulation	0.0	86	0.8	3368234	10 k	86	3416299	10 k
Media Type	0.1	396	7.3	31130328	93 k	396	31220487	94 k

Figure 12: Protocol Hierarchy of AAUA wireless Network

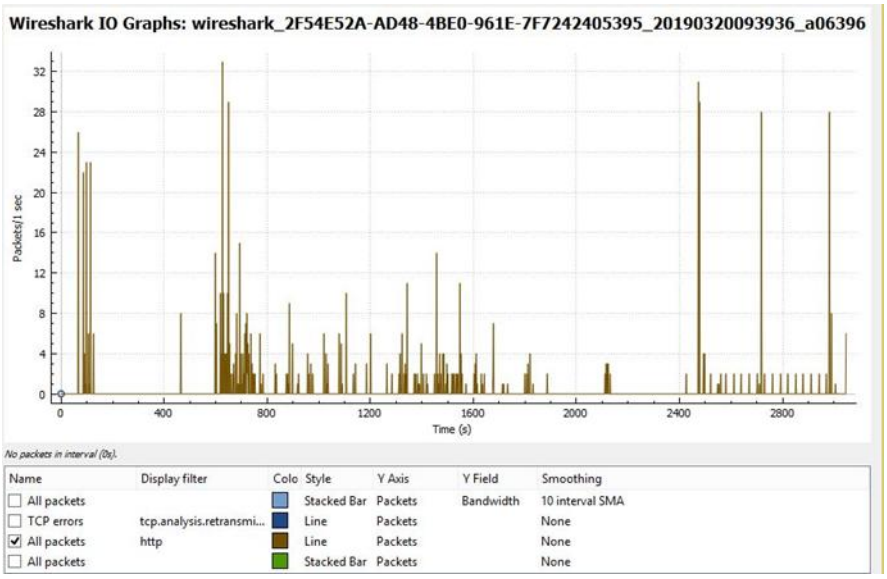


Figure 13: Network Packet Loss of AAUA wireless Network

VI. CONCLUSION

This paperanalyzes network usability patterns, user behavior, and bandwidth level of devices and application communicating over the network by considering specific QoS metrics in an autonomous network system using AdekunleAjasin University WLAN as a case study. By setting up a monitoring framework for data collection, processing, and visualizing, a systematic method was successfully built up to store traffic data, then to perform measurements and analysis. The Software based method of traffic measurement was adopted and a passive tool or sniffer (wireshark Network Analyzer) was used to sporadically poll the network. The tools used in this work are open sourced in order to realize an easy and common way for future work in traffic analysis. The results obtained were based upon statistical analysis of a large amount of data (network traffic). Thus traffic to and fro of the monitored network from various destinations was collected and classified based upon the location of the source/destination. In this way, the traffic characteristics of communication between the local network and networks user were effectively analyzed.

ACKNOWLEDGEMENT

The author acknowledge the technical contributions of the co-authors and also data collection. All authors read the final manuscript.

REFERENCES

[1] Adya, A., Bahl, P. and Qiu, L. (2002), Characterizing Alert and Browse Services for Mobile Clients. USENIX Technology Conference. 343–356. 2002.

[2] Arun, K.S., Ananya, B., Bhoomika, H., Ishan. S. and Krupal, S. (2018). Analysis of Network Traffic and Security through Log aggregation. International Journal of Computer Science and Information Security (IJCSIS). 16(6)

[3] Balachandran, A., Voelker G. M., Bahl, P., and Rangan, P. V. (2002). Characterizing user behavior and network performance in a public wireless LAN. Proceedings of the 2002 ACM SIGMETRICS Conference, Canada. 195–205.

[4] Bansal, R.K., Gupta, V. and Malhotra, R. (2010). Performance Analysis of Wired and Wireless LAN Using Soft Computing Techniques- A Review. Global Journal of Computer Science and Technology.10(8). 67-71

[5] Blinn, D. P., Henderson, T. and Kotz, D. (2005). Analysis of a Wi-Fi hotspot network. Proceedings of the International Workshop on Wireless Traffic Measurements and Modeling (WiTMeMo ’05).USENIX Association, June 2005, 1–6.

[6] Chandrashekar, K., and Janes, P. (2009). Optimal Design of Wireless Local Area Networks (Wlans) using Simulation. MILCOM 2009 - 2009 IEEE Military Communications Conference. doi:10.1109/milcom.2009.5380129

[7] Chuvak, A. and Surovtsova, T. (2018). Analysis of User Activity in Wireless Local Area Network of Petrozavodsk State University. Proceeding of the 22nd Conference of Fruct Association. 34-39

[8] Divgi, G. and Chlebus, E. (2007). User and Traffic Characteristics of a Commercial Nationwide Wi-Fi Hotspot Network. 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07). 1-5. Doi:10.1109/PIMRC.2007.4394305

[9] Kotz, D., and Essien, K. (2002). Analysis of a Campus-Wide Wireless Network. Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom), September 2002. 107–118.

[10] Lee, H.J., Kim, M.S., Hong, J.W. and Lee, G.H. (2002) "QoS Parameters to Network Performance Metrics Mapping for SLA Monitoring", *KNOM Review*, 5(2).42-53.

[11] Mistry, D., Modi, P., Deokule, K., Patel, A., Patki, H., &Abuzaghleh, O. (2016). Network traffic measurement and analysis. 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT). 1-7. doi:10.1109/lisat.2016.7494141

[12] Soldo, I. and Malarić, K., (2013). Wi-Fi Parameter Measurements and Analysis. MEASUREMENT 2013, Proceedings of the 9th International Conference, Smolenice, Slovakia. 339-342.

[13] Sulaiman, N. andYaakub, C.Y., (2010). Investigation on QoS of Campus-wide WiFi Networks. Journal of Telecommunications, 2(1). 12-16

[14] Tang, D. and Baker, M. (2002). Analysis of a Metropolitan-Area Wireless Network”. Wireless Networks. Proceedings of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking. 13-23. DOI=http://dx.doi.org/10.1023/A:1013739407600

[15] Wierenga, K. and Florio, L. (2005).Eduroam: past, present and future. Proceedings of Terena Networking Conference, Poznan, Poland, 2005. 169-173.