# MESH NETWORK OPERATING CENTER

**[1]S. KHALID, [2]A. SAUD, [3]M. OMAR, [4]M. USMAN, [5]S. S. KHAN, [6]S. LARKIN**

[1,2,3,4]Technosense21, Islamabad, 44000, Pakistan
[5]National Transmission and Dispatch Company Limited, Islamabad, 44000, Pakistan
[6]Africa New Energies Limited, London, 522416, United Kingdom
E-mail: [1]saadk2541@gmail.com, [2]abdullahsaud938@gmail.com, [3]omar@ts21.tech, [5]saadkhanopf@gmail.com, [6]Stephen.larkin@ane.na

**Abstract** - Network Operating Center (NOC) is a centralized location used by large enterprises to monitor their network for sustainability. This study proposes a robust design of mesh NOC that utilizes Raspberry Pi as a central monitoring and control unit performing different tasks, including Network Quality of Service (QoS) monitoring, Logging and Network Offloading. Real-time testing of the system under dynamic load was performed. The system was robust enough to maintain standard QoS levels by performing offloading techniques.

**Keywords** - Mesh Network, NOC, Network Offloading, Throughput, Bandwidth

## I. INTRODUCTION

Advancements in network technology have enabled users in a sophisticated or global network to access different types of information. This easy access to information has made the private data of various organizations vulnerable. Moreover, due to increasing number of users in the network also causes the availability of excess data or traffic in specific network channels leading to offloading problems **Error! Reference source not found.**. To handle such extensive data, network-providing enterprises provide a centralized location to monitor the incoming traffic from different channels, known as Network Operating Center. The NOC's most crucial role is to provide complete visibility into the enterprise infrastructure and all its components and equipment, including the following **Error! Reference source not found.**:

- Firewalls
- Network devices
- Servers
- Wireless systems
- Internet of things devices
- Virtual Machines (VMs)
- Databases
- Software and services (internal and external)

In addition, NOC personnel monitor and oversee network activity reports and dashboards. They may also attend to customer help desk systems ticketing-based, voice-based, etc. The NOC may integrate with customers' network tools to address customer service and support gaps. Consequently, the NOC plays an integral part in improving the company's customer focus and customer experiences. Consequently, the NOC plays an essential role in enhancing the company's customer focus and, ultimately, in improving customer experiences. From a security perspective, the NOC functions as the organization to monitor security and recognize and address any attacks or disruptions to the network. The NOC plays a critical role in maintaining uninterrupted network availability and, thus, Operational and business continuity.

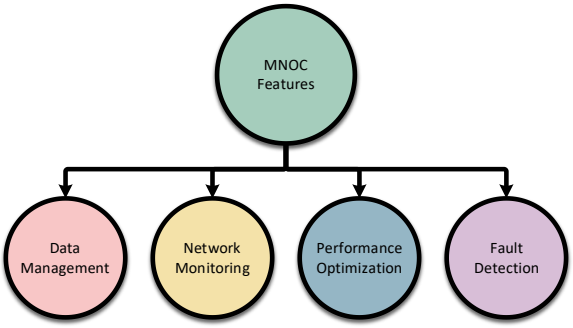



**Fig. 1. Features of Mesh Network Operating Center**

Datacenter hosts and manages the organization's data and supports enterprise operations through the proper collection, storage, protection, and distribution of data. NOC is often confused with Security Operations Center (SOC) and data center **Error! Reference source not found.**. Although the three are different from each other but in large organizations, they go on hand in hand; one is not possible without the other two. Companies having proper NOC, either internal or external, can expect to realize benefits like malware support, adequate handling of business-network critical software, optimization support, etc. Still, the function of the NOC is only to monitor and manage network operations while SOC personnel monitor the network for vulnerabilities, attack vectors, and threats. Mesh network-based network operation center is proposed, as shown in Fig. 1. to perform tasks like data management, network monitoring, performance optimization, fault detection and network quality parameters. Some existing methodologies for NOC include an RL model that can autonomously self-drive a lab network from raw data; a model can learn new implicit and nontrivial rules on its own, exceeding human performance with expert rules. RL model requires a lot of learning before achieving 100% performance [4,5]; a GSM-based Short Message

Service (SMS) notification system (ezzzyNotifier) with a shift timetable arrangement was designed to efficiently run a NOC in times of power outages or restorations. A system test revealed that it functions satisfactorily, with an average user satisfaction rating of 87% [6].

In this study, a robust mesh network operating center has been proposed. Section II will discuss the overall system design. The topic of section III is the real-time integration of the system, its testing and debugging. Section IV concludes the findings.

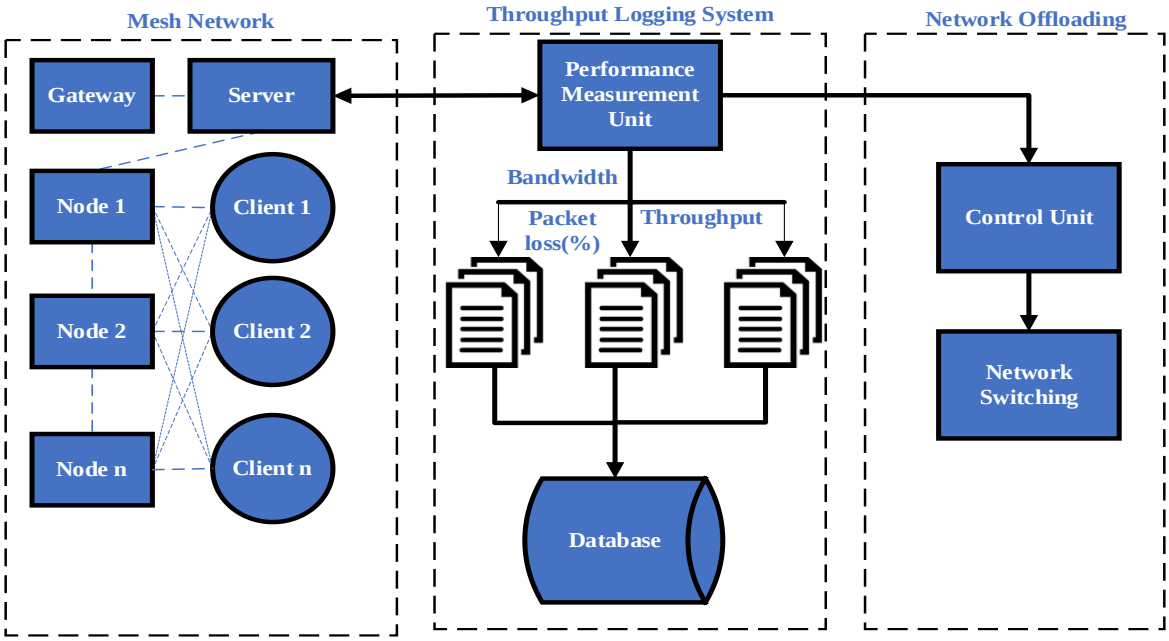



**Fig. 1. Overview of Proposed Mesh Network Operating Center**

## II. SYSTEM DESIGN

Overall system design consists of three operational blocks, as shown in Fig. 2. The mesh network performance block consists of servers and attached clients/devices. The server performance monitoring unit constitutes a logging system to log quality of service (QoS) parameters **Error! Reference source not found.** and transmit them to a linked database. Monitored parametric values help control units to make robust network quality by network offloading techniques. Mesh network contains gateway and nodes mesh to provide the self-organizing network with uninterrupted internet availability. In the proposed system, constrained devices are used for the infrastructure of the whole mesh network, including significant servers and attached nodes. A performance measurement unit extracts data from the server and processes it on the network performance measurement tools or software to monitor the parameters like Bandwidth, Throughput **Error! Reference source not found.**, Jitter (delay) and packet loss, etc. The Control Unit is equipped with algorithmic improvements to the network's performance to switch in an environment with maximal data consumption.

The following components are utilized for the real-time deployment of the proposed system.

- Constraint devices (Raspberry Pi)
- Client devices (Laptop/PCs, IoT devices)

### *A. Constraint Devices (Raspberry Pi)*

Raspberry Pi is utilized as the central server or decision body that monitors the performance of different channels in the network and analyzes the whole network performance. The Raspberry Pi development board comes with a built-in Wi-Fi module that can be configured in two ways:

- Using the Command Line Interface (CLI)
- Using the OS-provided Graphical User Interface (GUI)

Two options are available for adjusting the network settings through the command line. wpa-supplicant is a piece of supporting software that communicates with the Wi-Fi module to set up the network. This program requires a wpa-passphrase to be included in the configuration file wpa-suplicant.conf. After entering the necessary credentials, wpa supplicant will allow the Raspberry Pi to connect to the network.

### *B. Client Devices (Laptop/PCs, IoT)*

A network channel is a pathway through which two devices communicate with each other in the network. Client devices are an essential part of a network. Network devices such as Laptops/PCs, IoT devices like raspberry pi, microcontrollers, etc. Central server communicates with client devices and monitors and analyses the network traffic on that specific channel.

Unnecessary traffic or increased load on a particular client enables the server to make decisions like offloading and increasing or decreasing signal strength on that channel. The wireless router acts as a gateway to the internet, the server, and the whole mesh network. The router will provide Wi-Fi to the entire arrangement of constrained and unconstrained network devices. Internet connection is about 35Mbps.

## III. SYSTEM INTEGRATION, TESTING AND DEBUGGING

A sophisticated network consisting of a server and multiple clients connected in the mesh topology has been utilized. Raspberry Pi is the central control unit that monitors the network performance with the help of a software utility. It performs decision-making tasks like network offloading, bandwidth rationing, etc. Different types of software utilities are available that can be used to monitor network performance. Parameters that define network performance:

1. Bandwidth,
2. Throughput,
3. Jitter,
4. Packet loss
5. Latency

Linux based software is utilized that provides the parameters mentioned above, following client-server topology. Since all the nodes are connected in a mesh network, the server can communicate directly or indirectly with each node. Moreover, the throughput at each node in the network affects or gets affected by other nodes. So, a single client-server communication using network performance unit gives information about the performance of the whole network. Fig. 4 shows the working of network performance unit. This unit utilizes UDP communication between any two devices connected in the network(client/server) to monitor the QoS parameters.

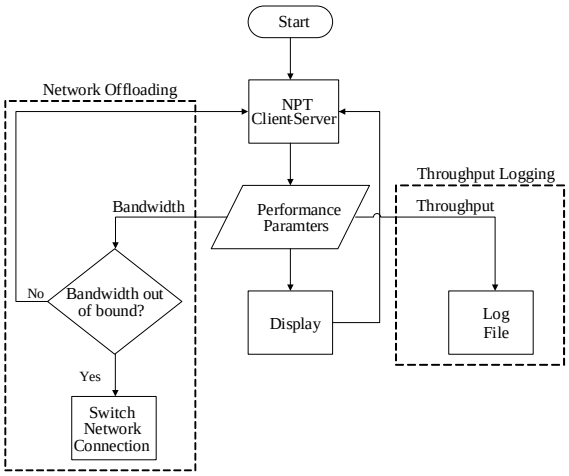


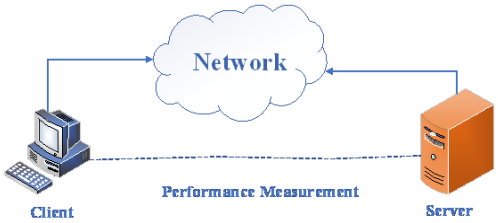

**Fig. 2. Working of Proposed Mesh Network Operating Center**

### *A. Algorithm development*

Fig. 3 shows the working of the proposed mesh network operating center. The system starts with the user's request to gather data from a specific network port. Any active node in the network sends a communication request to the server, which transmits packets at regular intervals of the defined monitoring time**Error! Reference source not found.**. The server can take decisions based on the measured parameters. After this, a complete summary of the performance report can be visualized through the monitoring window.

In a mesh network, each device is connected to all other devices in the network. So, the throughput of a single channel gets affected by the throughput consumed by other devices in the network. The network performance unit recognizes one node as a server and the other as a client. Depending upon the network protocol and permissions, the client sends packets to the server for a defined interval. The amount of data sent or received by the client or server is known as the throughput. Recorded throughput is logged and visualized through a database only concerned authorities can access.

The logging system starts with client-server communication performed by the network performance unit, measuring the throughput resulting from the transmission and logging the throughput data for a specified time interval. The priority-based bandwidth rationing algorithm is finalized by monitoring different data rates of the network. When bandwidth fluctuates and offloads a connected network device, the rationing algorithm **Error! Reference source not found.** will change the default gateway connection and restore bandwidth reduction. In this way, whole mesh network will re-organize itself for better QoS.

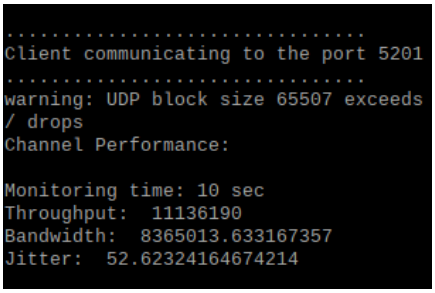



(a)

```
-----------------------------------
Server Listening to the port 5201
-----------------------------------
Channel Performance:

Client_Address:  192.168.1.32
Monitoring Interval: 10 sec
Throughput:  1318912
Bandwidth:  1048954.3973717538
Jitter:  0
```

(b)



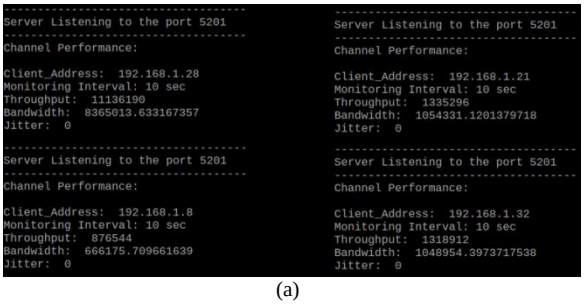

(c)

**Fig. 4. Working of Performance Measurement Unit**

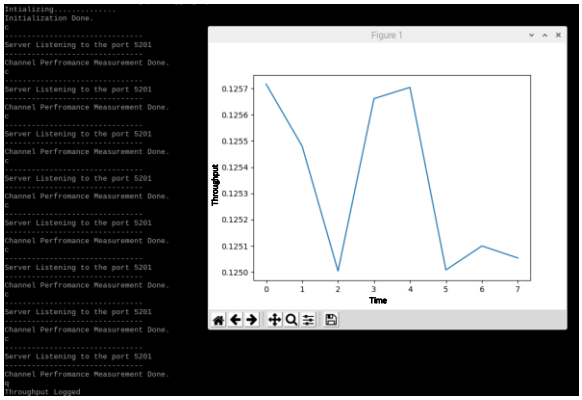
### *B. Testing and Debugging*

Iterative testing has been performed to improve the efficiency of the system. It has been observed from the experimentation, as shown in Fig. 5, that the network's throughput depends upon the bandwidth of the channel. Due to bandwidth shifting, variance has been observed in the logged data as throughput highly depends upon the channel's bandwidth, as illustrated in Fig. 5(a). So, it is important to log the channel's bandwidth along with the throughput. Moreover, a considerable delay has been observed while logging the data files into the database. In wireless communication, the distance of the client device or nodes from the server is inversely related to %packet loss in a specific channel. To increase the efficiency of such a throughput logging system, it is necessary to provide information on %packet loss along with the throughput.

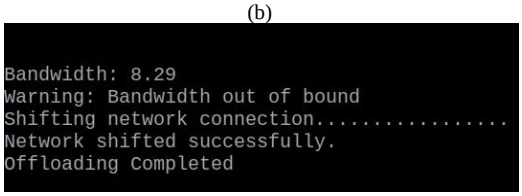
After the improvements mentioned above, the proposed system is much more efficient and wiser enough to monitor and log the throughput, bandwidth, and packet loss with the minimum possible delay. After integrating the whole proposed network, some of expected errors includes bad internet connection, poor client server communication and unexpected results while utilizing network performance unit and logging system errors due to bad software throughput utility from channels provided. To obtain encouraging results, the system will monitor client's IP address, bandwidth of specific channel, throughput of the channel, jitter in the channel. Network offloading will apply specific thresholds to the parameters in which exceeded bandwidth consumption shifts the network connection shown in Fig. 5(b). If throughput in the channel exceeds maximum capacity, i.e., bandwidth shrinks, the system can reduce throughput to maintain the overall load in the network.




(a)




(b)




(c)

**Fig. 5. (a) Results of Real-time Monitoring of QoS Parameters, (b) Results of Throughput logging Unit, (c) Results of Network Offloading Unit**

## IV. CONCLUSION

The proposed system comprises of constrained and unconstrained server-client mesh network. Network Operating Center (NOC) is a centralized location used by large enterprises to monitor their network for sustainability. A robust design of mesh NOC that utilizes raspberry Pi as a central monitoring and control unit performing different tasks, including Network Quality of Service (QoS) monitoring, Logging and Network Offloading. Real-time testing of the system under dynamic load made the system robust enough to maintain standard QoS levels by performing offloading techniques. This method enables consumers to continue using the internet even at high data rates.

## ACKNOWLEDGEMENT

The work is done under project code CMG026, funded by Africa New Energies Ltd, UK.

## REFERENCES

[1] Zhou, H., Wang, H., Chen, X., Li, X., & Xu, S. (2018). Data offloading techniques through vehicular ad hoc networks: A survey. IEEE Access, 6, 65250-65259.

[2] Raeisi and A. Giorgetti, "Software-based fast failure recovery in load balanced SDN-based datacenter networks," Proc. 6th Int. Conf. Inf. Commun. Manag. ICICM 2016, pp. 95–99, Dec. 2016, doi: 10.1109/INFOCOMAN.2016.7784222.

[3] Zimmerman, C. (2014). Cybersecurity operations center. The MITRE Corporation.

[4] R. Kanagavelu and Y. Zhu, "A pro-active and adaptive mechanism for fast failure recovery in SDN data centers," Adv. Intell. Syst. Comput., vol. 886, pp. 239–257, 2019, doi: 10.1007/978-3-030-03402-3_17/COVER.

[5] S. Wang, H. Xu, L. Huang, X. Yang, and J. Liu, "Fast recovery for single link failure with segment routing in SDNs," Proc. - 21st IEEE Int. Conf. High Perform. Comput. Commun. 17th

IEEE Int. Conf. Smart City 5th IEEE Int. Conf. Data Sci. Syst. HPCC/SmartCity/DSS 2019, pp. 2013–2018, Aug. 2019, doi: 10.1109/HPCC/SMARTCITY/DSS.2019.00278.

[6] G. Dimopoulos, I. Leontiadis, P. Barlet-Ros, K. Papagiannaki, and P. Steenkiste, "Identifying the root cause of video streaming issues on mobile devices," Proc. 11th ACM Conf. Emerg. Netw. Exp. Technol. Conex. 2015, Dec. 2015, doi: 10.1145/2716281.2836109.

[7] Rahane, S., Ulekar, S., Vatti, R., Meshram, T., & Male, S. (2018, March). Comparison of wireless network performance analysis tools. In 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT) (pp. 1-4). IEEE.

[8] Moudi, M., & Othman, M. (2020). On the relation between network throughput and delay curves. Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije, 61(3), 415-424.

[9] Patnaik Patnaikuni, D. R. (2017). A Comparative Study of Arduino, Raspberry Pi and ESP8266 as IoT Development Board. International Journal of Advanced Research in Computer Science, 8(5).

[10] Svoboda, J., Ghafir, I., & Prenosil, V. (2015). Network monitoring approaches: An overview. Int J Adv Comput Netw Secur, 5(2), 88-93.

[11] Kalpana, V., & Karthik, S. (2018, February). Bandwidth Constrained Priority Based Routing Algorithm for Improving the Quality of Service in Mobile Ad hoc Networks. In 2018 International Conference on Soft-computing and Network Security (ICSNS) (pp. 1-8). IEEE.

★★★