**ORIGINAL RESEARCH ARTICLE**

# eMobile internet protocol version six (IPv6) testbed for interoperability of Nigerian education services and networks

Oluwashola D. Adeniji

**Affiliation**
Department of Computer Science, University of Ibadan, Ibadan, Nigeria

***For Correspondence**
**Email:** od.adeniji@ui.edu.ng, sholaniji@yahoo.com; **Tel:** (+234) 706 537 0344

**Abstract**
The diversity of educational methods, services and protocols promoted disparate educational services in Nigeria. The diversity has not promoted resource sharing and has encouraged duplication of efforts. There is no doubt that the University systems in Nigeria need to complement each other bearing in mind the limited resources available to individual University system. With the introduction of next generation internet protocol version six (IPv6), some of the divergent technologies can be brought to a platform to facilitate resource sharing, capacity development and optimization of resources. In order to solve these diversities of resources affecting Nigerian Education Services and Network, Route Optimization Techniques in IPv6 will provide the best option for scaling these diversities. The Nigeria ecosystem has come of age and attained maturity level to identify the futuristic roles of internet protocol version six (IPv6). Globally, Policy makers and Governments have recognized the enormous opportunities the Internet can create and its impact on economic growth and prosperity. The prime mission of the invention is to develop and provide an eMobile IPv6 testbed that supports optimization of resources for digital services in Nigeria Tertiary Education**.**

**Keywords:** *Internet Protocol Version Six (IPv6), interoperability, services*

## Introduction

The term "MIPv6" is used to describe Mobile Internet Protocol Version Six (MIPV6). MIPv6 is a standard communication protocol that was developed by Internet Engineering Task Force. This communication protocol allows mobile device users to move from one network to another while maintaining a permanent Internet Protocol address. The dual role played by Internet Protocol (IP) addresses imposes some restrictions during mobility, because when a terminal moves from one network (IP subnet) to another, it will *maintain* the IP address of the node that is associated with in order not to change the identifier in the upper layers during ongoing sessions. The usage of Internet Protocol as a transport technology solves several interworking problems between different technologies. Wireless devices like handheld, PDAs, radios and others will have their own unique IP addresses. They will connect and communicate through their IP addresses. The new version of Internet Protocol, IPv6 provides enough IP addresses for these purposes. In Mobile IPv6, there are three mechanisms that support the mobility of a host: (i) movement detection, (ii) location registration and (iii) traffic tunneling. Movement detection is a process in which the Mobile IPv6 host discovers its own movement, and it requires an operation called router advertisement through a router. In other words, a change in the host or a mobile node's point of attachment to the Internet such that it is no longer connected to the same link in its previous connection. Mobile nodes detect their own movement by learning the presence of new routers as the mobile node moves into wireless transmission range. In order for a mobile node to operate correctly while away from home, at least one IPv6 router on the mobile node's home link must function as a home agent for the mobile node. Location registration is when a host or mobile node (MN) moves to a new network, it has to configure a new IPv6 address on the visited link (the IPv6 address space of that visited network). Traffic tunneling is when the MN has successfully registered its current location and the home agent starts encapsulating the data traffic destined to the mobile node toward its care of address (CoA).

**Literature Review**

The new practice of the internet will be related to the ubiquitous version of the internet with billions of heterogeneous devices connected together. The standard in mobility management is the mobile IP. To support IP mobility, Internet Engineering Task Force (IETF) has proposed Mobile IP based on IPv4 and IPv6, to solve most of the problems facing mobility issues. The review report in [1] provides observation in a test bed experiment of three level hierarchies in MIPv6 with optimal performance of 27% in handoff latency. The Home Agent replies to the mobile node by returning a "Binding Acknowledgement" message. Like the Binding Update, Binding Acknowledgment is encoded as an option to be carried within a Destination Options Header in [2,3]. The prediction of incoming attacks is achieved in a timely manner which enables security professionals to install defense systems in order to reduce the possibility of such attacks in [4] was proposed in Zero Day attack Prediction. The purpose of this paper is to present, in detail, the deployment of a simple and cost-effective Linux-based Mobile IPv6 Testbed for the study of handover execution with testing checkpoints and debugging procedures. Further, this paper evaluates performance metrics such as bandwidth, packet delay, jitter and handover delay with respect to TCP and UDP traffic and compares the same with the MIPv6 NS2 simulation results in [5] are essential in information security. The tradeoff between the two protocols can provide a significant impact on the networks in [6]. The significant roles of encryption algorithms are numerous and essential in information security as reviewed in [7] Comparative Study of Symmetric Cryptography Mechanism. *The **Interoperability** of GSM networks have already evolved to 3G, 4G, LTE, 5G and data speeds are improving with High-Speed Downlink Packet Access (HSDPA), HSDPA+ etc.* thereby making data access on mobile very comfortable. IPv6 compliance testing on mobile handsets using RFC 3314 and 3316 is performed on the eMobile IPv6 testbed. The wire line broadband CPEs shall be capable of carrying IPv6 traffic either on dual stack or on native IPv6. Broadband evolution will ride on IPv6 resulting in an exponential demand of IPv6 ready end user devices. The benefits of Mobile IPv6 compared to Mobile IPv4 include: Large address space, Address Auto Configuration, Dynamic Home Agent Discovery, Built-in Security*:* Mobile IPv6 makes use of the IPSec for all security requirements like authentication, data integrity protection and replay protection. Route optimization: Mobile IPv6 avoids so-called triangular routing of packets from a Correspondent Node to the Mobile Node via the Home Agent. The nature of wireless communication, including mobile IPv6 that broadcasts messages to receivers, is explicitly prone to malicious attacks [8]. The attacks could be eavesdropping [8], DoS (denial of services) [9], spoofing [10], MiTM (Man in the Middle) [11], and falsification [12]. The 2016 Norton cybercrime [13] report stated 87% of consumers have in-home Wi-Fi, and they engage in dangerous behaviours. However, there are no adequate provision for quality of service (QoS) in OpenFlow using Flow Label to reduce bits required as a field to match packets in internet protocol six (IPv6) [14].

## Methodology

A complete discussion of the procedure, layout and configuration process for implementing the testbed is presented. *The strategy and approach of the method are divided in three phases.*

***In phase 1**, the solution is to develop Mobile IPv6 implementation based on MIPL (MobileIPv6 Platform for Linux). The phase consists of topology configuration and setup of node based on specified requirement. The interconnectivity of network in the testbed for MIPV6 required node keys 1,2,3,4, which are Home Agent (HA), Correspondence Route (CR), Correspondence Note (CN), Mobile Note (MN) unlike in the previous invention in which bi-directional tunnel was used has a mode of communication and candidate Route optimization was not considered as presented below.*

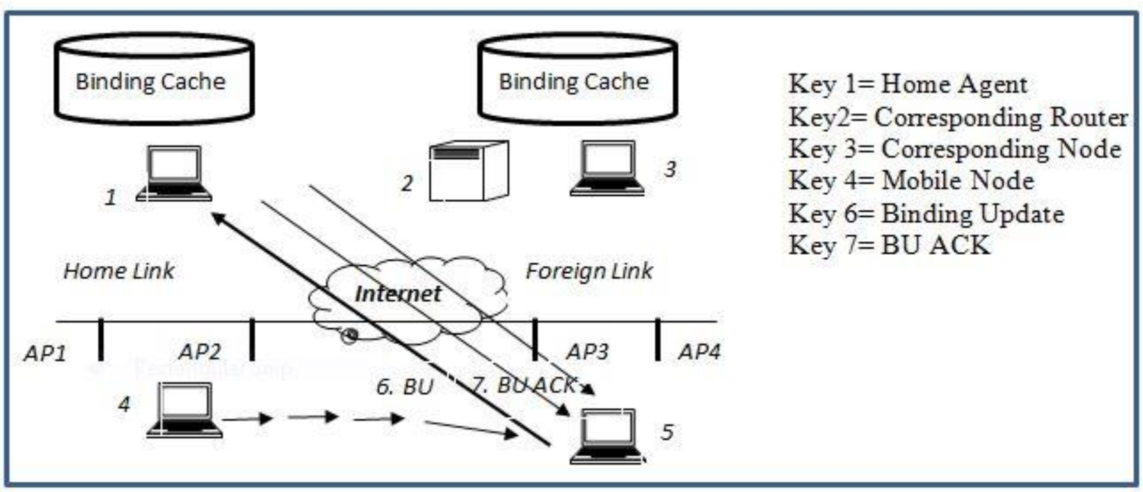


**Figure 1: Phase 1 development of the Testbed**

Whenever the MN moves to a different access network, it informs the HA of its new care-of address configured on the link by sending a Binding Update. When the HA receives this message, it returns a Binding Acknowledgement (Binding Ack). Packets from the MN are tunneled to its HA where the HA forwards the packet to the CN. HA must maintain a database to manage the MN it is serving. This database is called the Binding Cache.

***Phase 2****: The development in Network Mobility implementation is based on the NEPL (NEMO Platform for Linux). The operation in NEMO require node 4 which is mobile router (MR) and is similar with the MN of Mobile IPv6. A MR is provided with a home address which is allocated from the home link of its HA. The diagram below shows the implementation.*

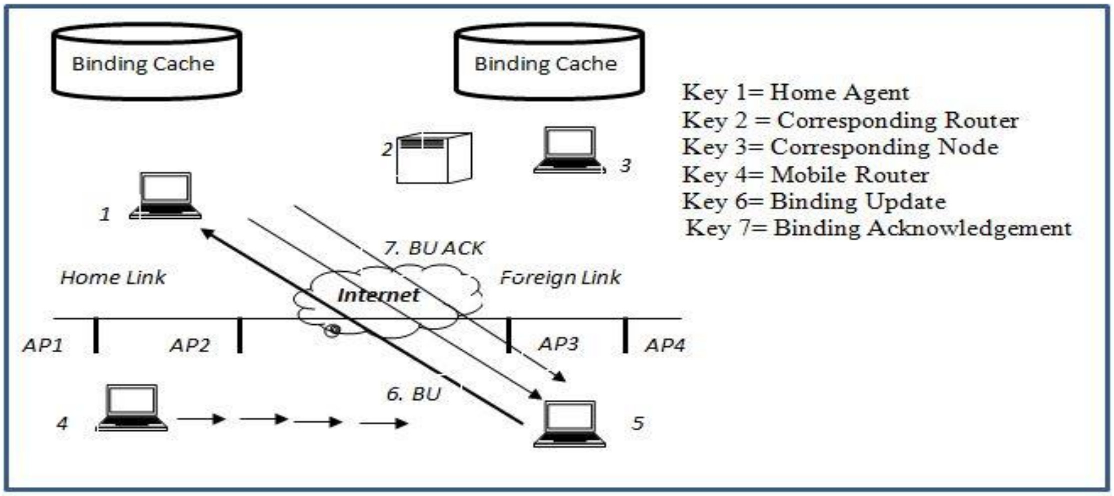


**Figure 2: Phase 2 development of the Testbed**

MR configures the care-of address after moving into a new access network, it notifies the change to its HA by sending a Binding Update message, 1 in Figure 2 The Binding Update message includes the home address and the MNP and is sent with the care-of address as the source address. The HA updates the corresponding entry in its Binding Cache with the new care-of address and returns a Binding Acknowledgement (Binding Ack) to the MR 2 in Figure 2. The Binding Ack is sent to indicate the registration status of the Binding Update of the MR.

***Phase 3 involve the*** *development of hybridize algorithm for route optimization protocol in IPv6 and network mobility (NEMO). In this phase, the packets that are forwarded via the HA may lead to suboptimal path depending on the location of the MN, CN and the HA.*

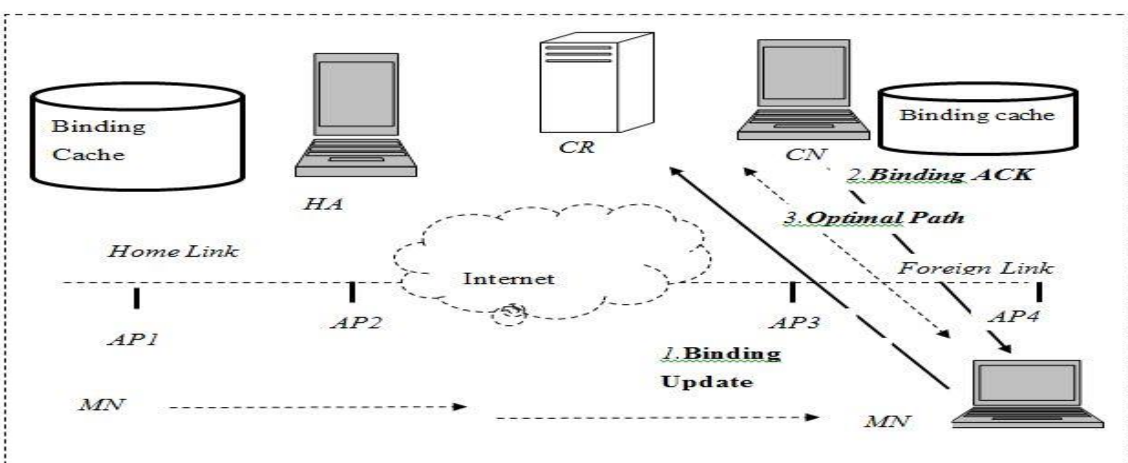


**Figure 3: Phase 3 development of the Testbed**

When the MN receives a packet forwarded from is HA, it triggers to perform route optimization with the CN .MN first processes the Return Routability procedure defined in the specification and then sends a Binding Update to the CN. When the CN receives this message, it returns a Binding Ack to the MN. After a successful establishment of the bindings, packets are forwarded directly using the optimal path (3 in fig 3) with the newly defined mobility headers and routing headers. The figures 4 and 5 below show the results in the kernel compilation process and make install process and Care-of-Test, Router Solicitation and Neighbor Advertisement.

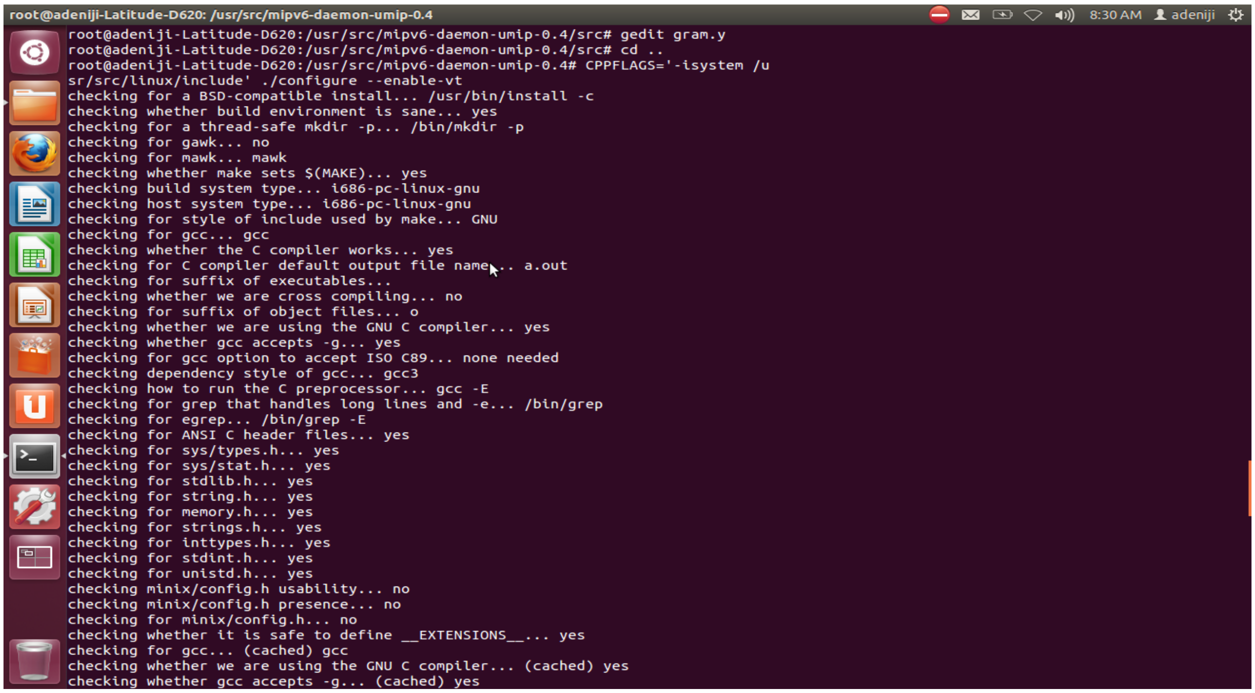


**Figure 4: Kernel Log Configuration and Compilation Process**

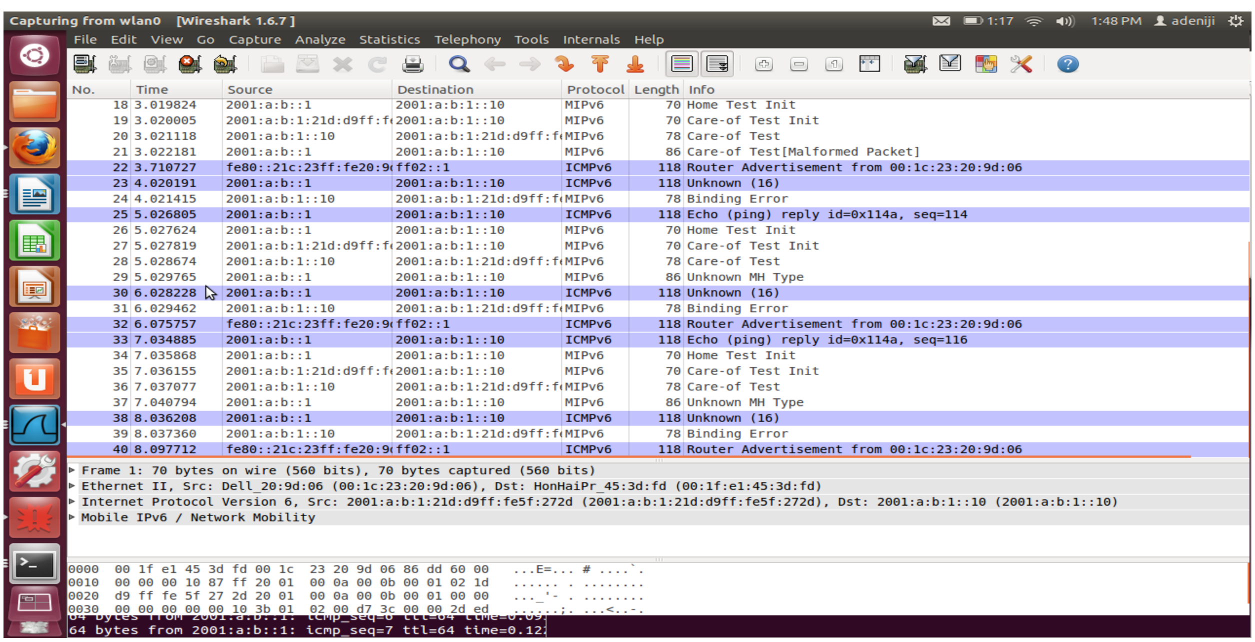


**Figure 5: MNN Roam to AP1 showing Care-of-Test, Router Solicitation and Neighbor Advertisement**

The characteristic of hardware and software specification used for computation in the testbed experiment is shown below in Table 1.

**Table 1: Specification of Hardware and Software for the Testbed Design**

| S/N | Nodes | CPU/Speed | Kernel Configuration | Platform | *OS* |
|---|---|---|---|---|---|
| 1 | HA | Core TM 2CPUT5500@ 1.66GHZ 1.67 GHZ | Kernel Linux 2.6.29.5 | MIPv6/NEMO Platform | OS: 32 Bit |
| 2 | MR | Core TM 2CPUT5500@ 1.66GHZ 1.67 GHZ | Kernel Linux 2.6.29.5 | NEMO Platform for Linux (NEPL) | OS: 32 Bit |
| 3 | MNN | Core TM 2CPUT5500@ 1.66GHZ 1.67 GHZ | Kernel Linux 2.6.29.5 | Mobile IPv6 Platform for Linux (MIPL) | OS: 32 Bit |
| 4 | CN | Core TM 2CPUT5500@ 1.66GHZ 1.67 GHZ | Kernel Linux 2.6.32 | Not Required | OS: 32 Bit |
| 5 | CR | Dual-Core T4500 @2.30GHZ 2.30GHZ | Kernel Linux 2.6.29.25 | Not Required | OS: 32 Bit |

**Discussion of Result**

The real implementation of MIPV6 and NEMO was carried out based on wireless standard IEEE 802.11b. MIPV6 and NEMO were combined for effectiveness during the experiment. Prior to the starting of the testbed and measuring the performance, time synchronization with Network Time Protocol (NTP) was performed in order to guarantee accuracy of the results. The figure below shows the result of the developed platform.

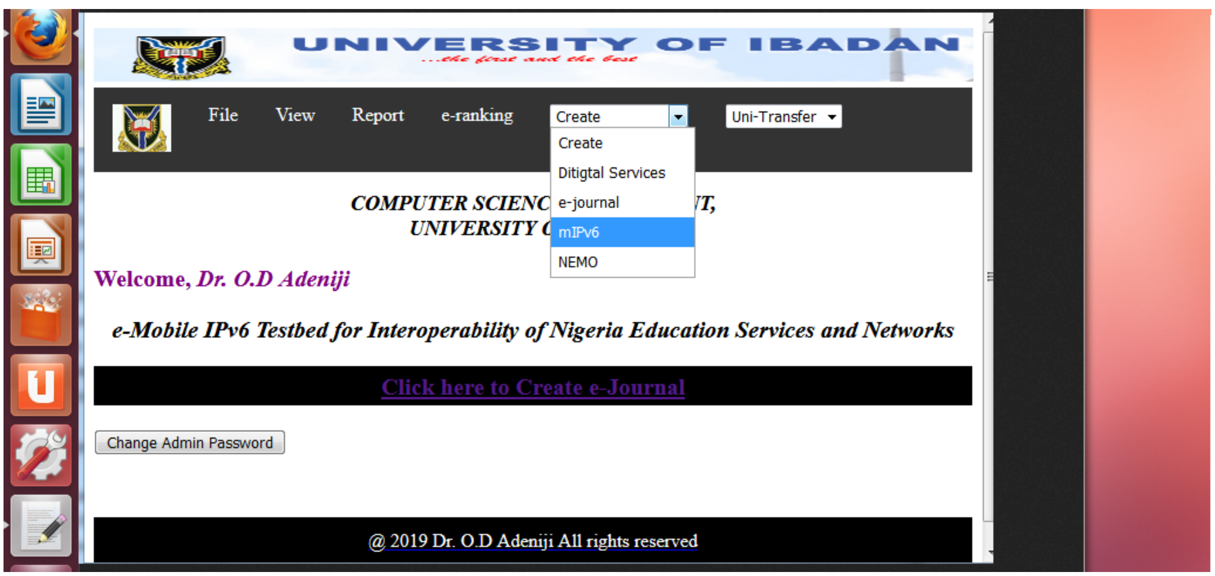


**Figure 6: e-Mobile IPv6 Testbed Platform**

*The result from the platform shows information on university uni-Transfer, e-journal-ranking, and digital service. Nigeria Universities need to coexist and collaborate in order to share these resources. Based on the platform developed streaming of video was conducted using* User Data Protocol (UDP). *Digital services that deploy application for* UDP *was configured and tested on the developed platform. Software defines network, Network slice, network virtualization can be deployed on the developed platform.* UDP is a connectionless protocol because of its stateless nature and that is why it is basically used to answer small queries from huge number of clients to server relationship. Also, UDP can broadcast and multicast packet during deployment. The movement of NEMO network from one train station to another will lead to temporarily dropped of packet with users. Application such as video stream can be affected. The figure below shows the result.

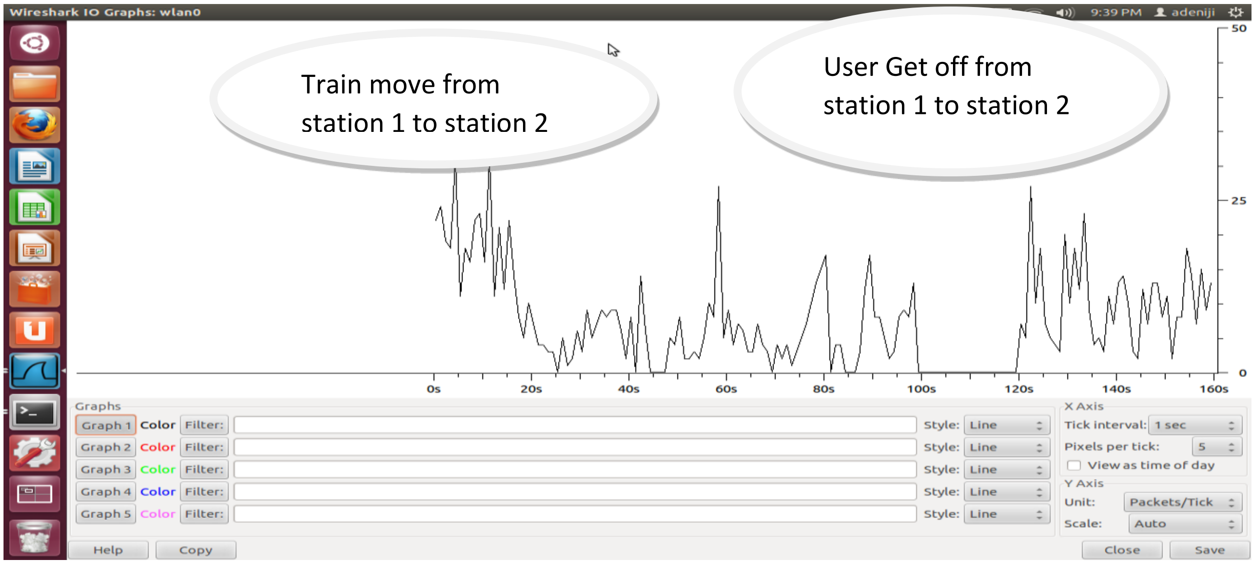


**Figure 7: UDP Video Stream of Implementation Test 1**

Basically, the stations referred to in the study are access point, MR will successfully register the BU with HA and receive BA when NEMO takes place. In streaming the video, packet will drop to zero. UDP packets are divided into small packet, and later reassemble again at the receiver. The observation in figure 7 only shows that between 42sec and 45sec the packet is divided and reassemble again as the train move. At 100sec and 110sec users get off from the station1.

## Conclusion

The developed innovation can provide exchange of digital services such as inter-university course transfer and objective global ranking of Nigeria tertiary education. It was observed that the requirement to provide IPv6 digital services was neglected. Platform to facilitate resource sharing, capacity development and resources optimization must be created. The only Tertiary institution in Nigeria with IPv6 digital services is university of Ibadan. This developed e mobile IPv6 in university of Ibadan will provide resource sharing of digital service in our educational sector. *The prime mission of the invention is to develop and provide eMobile IPv6 testbed that support optimization of resources for digital services in Nigeria Tertiary Education.*

## References


1. Dutta N, Saha IS Misra, Pokhrel R, & Mrinal K (2014). Performance Analysis of Multilayer MIPv6 Architecture through Experimental Test bed, Journal of Network, Vol 7, pp 1682-1691

2. Cho S, Na J, Kim C, Lee S, Kang H, & Koo C (2014). ‖Neighbor MR Authentication and Registration Mechanism in Multihomed Mobile Networks‖ IETF Internet Draft.

3. Atiquzzaman M, Shahriar AZM, & Ivancic W (2010). Route optimization in network mobility: Solutions, classification, comparison, and future research directions," IEEE Communications Surveys & Tutorials, Vol.12, No.1, pp.24-38.

4. Adeniji OD & Olatunji OO 2020. Zero Day Attack Prediction with Parameter Setting Using Bi Direction Recurrent Neural Network in Cyber Security. International Journal of Computer Science and Information Security (IJCSIS), Vol. 18, No. 3, pp 111-118.

5. Chandavarkar BR. Deployment of a Simple and Cost-Effective Mobile IPv6 Testbed for the Study of Handover Execution (2020). ICCCE 2020, Proceedings of the 3rd International Conference on Communications and Cyber Physical Engineering.

6. Adeniji OD & Osofisan A (2020). Route Optimization in MIPv6 Experimental Test bed for Network Mobility: Tradeoff Analysis and Evaluation. International Journal of Computer Science and Information Security (IJCSIS), Vol. 18, No. 5, pp 19-28.
7. Logunleko KB, Adeniji OD, & Logunleko AM (2020). A Comparative Study of Symmetric Cryptography Mechanism on DES, AES and EB64 for Information Security. International Journal of Scientific Research in Computer Science and Engineering Vol.8, Issue.1, pp.45-51.

8. Lakshmanan S, Tsao CL, Sivakumar R, & Sundaresan K (2008). Securing wireless data networks against eavesdropping using smart antennas," in *Proceedings of the. International Conference on Distributed Computing Systems ICDCS'08*, pp. 19–27, Bandung, Indonesia, 2008.

9. Raymond DR & Midkiff SF (2008). "Denial-of-service in wireless sensor networks: attacks and defenses," *IEEE Pervasive Computing*, vol. 7, no. 1

10. Kannhavong B (2007). "A survey of routing attacks in mobile ad hoc networks", *IEEE Wireless Communications*, vol. 14, no. 5.

11. Meyer U & Wetzel S (2004). "A man-in-the-middle attack on UMTS," in *Proceedings of the 3rd ACM Workshop on Wireless Security*, ACM, New York, NY, USA.

12. Ohigashi T & Morii M (2009). "A practical message falsification attack on WPA," *JWIS*, vol. 14, 2009.

13. Norton S (2016). "Norton cyber security insights report.

14. Olabisi AA, Adeniji OD, & Abeng E (2019). A Comparative Analysis of Latency, Jitter and Bandwidth of IPv6 Packets Using Flow Labels in Open Flow Switch in Software Defined Network‖ Afr. J. MIS, Vol.1, Issue 3, pp. 30-36.