Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 20 Issue 4 Version 1.0 Year 2020
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 ISSN Print 0975-4350

Enhancing Capacity and Network Performance of Client-Server Architectures using Mobile IPv6 Host-based Network Protocol

By Ruphin Kusinza Byamungu
Hope Africa University

Abstract- A huge number of studies have been done supporting seamless mobility networks and mobile technologies over the years. The recent innovations in technology have unveiled another revolution from the static architectural approach to more dynamic and even mobile approaches for client-server networks. Due to the special equipments and infrastructure needed to support network mobility management, it is difficult to deploy such networks beyond the local network coverage without interruption of communications. Therefore, MIPv6 as developed by the Internet Engineering Task Force (IETF) and ancillary technologies were reviewed to provide clear insights on implementing MIPv6 in Client-Server architectures. However, MIPv6 technology presents weaknesses related to its critical handover latency which appears long for real-time applications such as Video Stream with potential loss of data packets during transmission.

Keywords: client-server; mobile IPv6; fast handover mobile IPv6; route optimization; IPSec; TCP; UDP.

GJCST-E Classification: C.2.2

Strictly as per the compliance and regulations of:

Enhancing Capacity and Network Performance of Client-Server Architectures using Mobile IPv6 Host-based Network Protocol

Ruphin Kusinza Byamungu

Abstract- A huge number of studies have been done supporting seamless mobility networks and mobile technologies over the years. The recent innovations in technology have unveiled another revolution from the static architectural approach to more dynamic and even mobile approaches for client-server networks. Due to the special equipments and infrastructure needed to support network mobility management, it is difficult to deploy such networks beyond the local network coverage without interruption of communications. Therefore, MIPv6 as developed by the Internet Engineering Task Force (IETF) and ancillary technologies were reviewed to provide clear insights on implementing MIPv6 in Client-Server architectures. However, MIPv6 technology presents weaknesses related to its critical handover latency which appears long for real-time applications such as Video Stream with potential loss of data packets during transmission. Therefore, the research exploited Fast Handover MIPv6 solution introduced by IETF under Request for Comment (RFC) 5268. This protocol maintained the technological capacity of MIPv6 such as (Internet Protocol Security (IPSec) and Rout Optimization (RO) to name a few, but also provided faster Binding Updates between the Client or Mobile Node (MN) and its Home Agent (HA) which improved on the overall network performance. To implement the proposed solution, Discrete Event Simulation (DES) method was adapted using OMNET++ with INET Framework where application service models such as File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP) and Video Stream were implemented based on a dynamic bitrate selection mode under IEEE 802.11g. The performance was measure based on different network performance metrics such as Handover Delay, End-to-End Delay, Throughput, Packet Error Rate and Packet Loss Rate based on both TCP and UDP transmission protocols. The research involved a comparative analysis approach between MIPv6 and FMIPv6 in the analysis of the collected data. Based on the results produced, FMIPv6 shows a better network performance and much better Quality of Service than MIPv6.

Keywords: client-server; mobile IPv6; fast handover mobile IPv6; route optimization; IPSec; TCP; UDP.

Categories: Computer Networks and Communication

Author: Computer Science Department, Telecommunication Engineering and Management Department, Hope Africa University (Université Espoir d'Afrique), Bujumbura, Burundi.
e-mail: rkusinza@gmail.com

I. Introduction

In today's Internet and Information Systems resource use, people have struggled integrating the notion of mobile Internet technologies within the very crucial and sustainable technology areas such as the client-server. From individuals to corporations, mobility gap along with the lack of an extended application of the handover and roaming techniques introduces the main problem toward enabling servers and their clients to seamlessly transmit information to each other. There is a technical coexistence and compatibility between large coverage access networks such as GSM or GPRS/EDGE, UMTS and LTE with Local Area Networks (LANs) and dedicated short-range communications setups, making it possible for devices in both large and short-range coverage to exchange information and signals [1]. Hence, in resource intensive technologies such as client-server, two specific network architectures would meet specific capacity requirements [2]. These architectures include heterogeneous cellular networks where different coverage areas and technical capabilities are determined by the antenna transmission power, data throughput and network density parameters for a specific area of coverage. They also include heterogeneous radio access network architecture which requires internetworking and interoperability of different radio access technologies such as GPRS, WLAN, WiMAX, and LTE [3]. This process would allow IP networks to use cellular networks infrastructure in convergence with Voice communications complying to the infrastructure monopoly of cellular networks resources and the problematic potential consequences of converged technologies.

According to [2], most active wireless and mobile networking in the future will have Mobile IP (MIP) as their common and enabling technology. The expectations are that many technologies including client-server, and devices running a variety of applications will be deployed in a loosely coupled environment where IP will be playing the role of the unifying architectural environment. Both IPv4 and IPv6 are considered capable of offering significant capabilities into implementing Mobile IP technologies in private and public network settings, but IPv6 is usually chosen instead of IPv4 due to multiple aspects including

a wider range of address space availability which utilizes a 128-bit address versus 32-bit address in IPv4 and evolved network security optimization approach [4]. MIP technology concept which is of two categories including MIPv4 and MIPv6 offers path to the process of providing home network access to users by delivering a unique home network identity such as the IP address to the mobile user [5]. MIPv6 being the bull's eye of this research can be defined as a subset of IPv6 to support mobile connection. It is also seen as an update of the IETF Mobile IPv4 standard (FRC 2002) for authentication of Mobile Nodes (MN) using IPv6 [6].

The explosion of certain mobile applications, based on Internet Protocol such as web or hybrid applications involving protocols including HTTP (web services), FTP, Video Streaming is the latest example and driving force showing that mobile wireless network is now the focus of technologies such as distributed computing [7], and that to a certain extent would be applied in client-server environment. Users have embraced these technology advances with the proliferation of mobile computers in the form of laptops, palmtops and PDAs at its peak, and as important elements of the current computing environment. Research reveals another theoretical approach where client-server architecture in a mobile environment is related to its application in mobile multiplayer games where the server stores and processes all the game data sent by all the connected mobile clients. The server therefore, only updates the clients with the particular data they need anytime, anywhere [8].

a) Research Problem

Client-server architectures can be implemented in various kinds of technologies. But for users and clients to seamlessly remain connected to the server located over the internet even after leaving its current network or gateway, it requires a specific and reliable technology. Mobile Internet Protocol version 6 legitimately responded to the concern based on various technological standards and implementation capabilities of the technology in network architectures. Therefore, RFC 6275 Mobility Support in IPv6 was introduced by IETF in 2011 to practically prove and standardize the MIPv6 technology concept [9]. So, MIPv6 places itself at the idealistic position offering MNs possibility to seamlessly connect and exchange services with the CNs online regardless of their location, i.e. using different network identifications. Based on IP Security (IPSec) protocol, MIPv6 provides security assurance to networks and devices while it is possible to optimize the routing process through Route Optimization. However, the implementation of MIPv6 technology presents some technology weaknesses that are related to its critical handover latency which appears too long for real-time applications such as Video Stream with potential loss of data packets during transmission. Therefore, a technology with improved handover latency, acceptable security and optimized packet routing process would establish comfortable and reliable environments for nodes adhering to MIPv6-based networks. These environments may include client-server network architectures. This research is driven by one general objective and four specific objectives.

b) Research Objectives

The general objective of this study was to enhance capacity and network performance of client-server architectures using Mobile IP version 6, Host-based network mobility protocol. The research is expanded into four specific objectives:

- Evaluate MIPv6 technology and client-server network mobility problems though literature review and propose a solution framework.
- Design and implement client-server architecture using an optimized and secure MIPv6 solution in a simulated environment.
- Evaluate network Quality of Service of the implemented MIPv6 solution for FTP, HTTP and Video Stream services.
- Implement and evaluate client-server Fast Handover MIPv6 solution for better quality of service.

II. Review of the Literature

a) Research Background

In recent years, Mobile IP has been spread through different levels of application in a diverse number of technology applications and issues. But most of all, the notion has its grassroots from the late 90's where the Mobile IP working group in connivance with the IETF working group continued to upgrade features and technology parameters regarding novel requirements from individual to enterprise standpoint. IETF started focusing on the definition of a general AAA infrastructure (RFC 2977) that could be useful for true mobile communications, mostly to support Mobile IP Authentication, Authorization and Accounting. The draft used the model presented in Figure 1 with AAA Home Server and AAA Foreign Server with a middle Broker [10]. In the AAA framework processes in MIP, Home Agent and Foreign Agent in the Home network and the Foreign network, respectively are mobility management agents for the MN. Signals are exchanged between the three components before packets are delivered to a MN allowing an establishment of routing tables for future packet delivery to the MN [11]. In real-life implementation, security attacks such as eaves-dropping, man-in-the-middle and replay prompt security measures that could implement RADIUS of Diameter protocols to provide a centralized network access management based on the AAA concept [12].

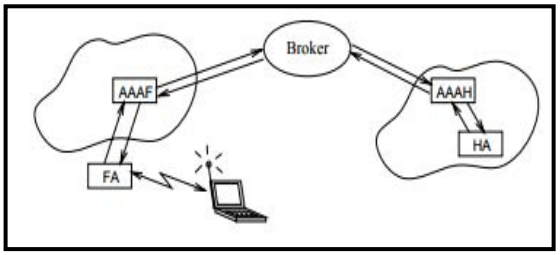

Figure 1: Mobile IP/AAA Framework [13]

This research introduces improved technological mobility measures with MIPv6 implemented in client-server architectures where MN is mostly in charge of the mobility management functions with a secure and optimized exchange of information with other network entities.

b) Network Mobility in Client-Server Architectures

Wireless technology revolutionized network concept by offering network users and entities such as PC and handheld phones freedom from the constraints of physical and wired network structures at a relatively low cost. This allows mobile users to exploit the technology at their fingertips. Based on wireless technologies such WLAN, WMAN, WWAN, etc., mobile technologies promised the principle of "anything, anytime" to users [14]. All these wireless technologies have however, contracted numerous limitations in terms of coverage range, mobility, infrastructure and others which could have a negative effect on user experience in client-server with limitations restricting clients from contacting the server [15]. However, MIPv6 present a prominent profile into filling the gap in solving problems surrounding these limitations in providing mobility and security capabilities to network devices, which could be helpful in client-server architectures. This protocol would as well provide security and independence to clients, hence host-based network, and expand the availability of services wherever and whenever possible while ensuring security to devices communicating. Implementing MIPv6 acquires more substance from the ability of IPv6 to provide address auto-configuration capacity to MN or the client as it moves across different networks [16].

c) Internet Protocol Version 6

IPv4 was the first widely deployed Internet protocol standardized about 25 years ago. This protocol suffered and continued suffering several design problems, which tend to restrain the creation of new usages of the Internet [17]. Among the issues surrounding this protocol are the lack of IP addresses that has had an impact on technologies such as Voice over IP (VoIP) that need more IP addresses to attribute to mobile users and limited security. The protocol is based on a 32-bit logical address which is a total of 4,294,967,296 billion unique addresses consisting of five classes, A, B, C, D and E [18].

Pv6 on the other hand outperforms IPv4 on many important issues where the main difference is that IPv6 has a larger address space with about 340 undecillion (2^{128}) IP addresses which is enough if we estimate that every human gets to use 3 IP address out of 7 billion people living on the earth (340 undecillion – 21 billion) and giving more reasons to migrate to IPv6 [19]. IPv6 also provide better security mandating that IPv6-enabled nodes must support the IPSec protocol, but also including payload encryption and authentication of the source of the communication. Furthermore, IPv6 provides extensibility since the protocol can be extended for new features just by adding extension headers. IPv6 also provide better QoS with support for real-time traffic such as VoIP that includes built-in "labeled flows" mechanism like the service offered by Multi-Protocol Label Switching (MPLS). Lastly, it facilitates the connection of entities to the network through its auto-configuration mechanism known as "plug-and-play" and called stateless auto-configuration that speeds up network connections mostly in large IPv6 network, and where router provides the network prefix from router advertisement to MNs, different from the stateful mechanism where DHCP server provides the address [19]. However, since IPv6 is considered the next generation of Internet technology, the constraints of legacy internet surrounding technology cost and change have incited the development of three transition and coexistence mechanisms between IPv4 and IPv6 that includes Dual-Stack, Tunneling and Translation mechanisms [20].

d) Mobile Internet Protocol Version 6

MIPv6 was developed as a subset of IPv6 to support mobile and seamless connections of mobile devices designed to authenticate and serve mobile devices using IPv6 protocol. The technology is thought of as the opening of the Mobile Internet Age. Therefore, following the current state and trend of Internet infrastructure, MIPv6 is overwhelmingly needed to provide not only internet and mobility services but also security to mobile devices [20] [21].

The following procedure explains the flow of operations that ensures a well-connected MN in MIPv6 environment. Indeed, MIPv6 offers a way for MNs to seamlessly preserve connectivity while travelling across different access networks or subnetworks [22]. Every MN is destined to have a Home Network (HN) with a permanent home IP address attributed to the MN. Additionally, in each HN we fin entities such as HA in charge of tracking MNs as they move from home to Foreign Networks (FN). MN received by the FN through a broadcasting Access Router (AR). So, once a MN leaves its home network and moves to the neighbor network or FN, it obtains a new IP address called Care-of Address (CoA). The MN is then required to register this new IP address (CoA) with its HA through a Binding

Update message which defends its authenticity, authorization, and integrity and that is issued over an IPsec protocol opening a secure bidirectional tunnel of communication between the MN and its HA. Thus, after the binding is received, the HA respond with a binding acknowledgement (BAck) so that even as the MN moves to a foreign network, a Correspondent Node (CN) can still maintain communication with the MN using 'indirect routing' that is made of packets being relayed by the HA [23]. This process creates a time of inactivity that is referred to as handover time or handover latency. Therefore, MIPv6 makes use of triangular routing and route optimization to forward packets to and from the MN [18]. Route Optimization (RO) is used to decrease signaling overhead at the border router and to offer a way for both MN and CN to forward packets to each other directly without sending or receiving them from HA. With MIPv6 if there are no security mechanisms such as IPsec, and Return Routability, CN does not know which MN sent the BU [24]. However, the BU is not secret, but it always needs to be sent from a legitimate MN.

The main issue with MIPv6 is the handover delay when MN is moving between networks. Handover latency is affected by a process made of several components [25]:

Link Layer Establishment Delay (DL2): Required time by the network nodes' physical interfaces to establish a new association with the visiting client or MN. This is the L2 handover between AP linked to different access routers.

Movement Detection (DRD): Time required for the MN to receive wireless beacons from the new AP, after disconnecting from the old AP or the old access network.

Duplicate Address Detection (DDAD): handled by the network router. It indicates time required to recognize the uniqueness of the mobile IPv6address within the home network.

Binding Update/Registration Delay (DREG): is the time elapsed between the sending of the Binding Update from the MN to the HA and the transmission/reception of the first packet through the new AR (FA).

The process is represented in the following equation:

$$DMIPv6 = DL2 + DRD + DDAD + DREG \quad (1)$$

According to [25], we can still break the delays down to:

$$DMIPv6 = (TPRB + TAUTH + TRASS) + (TRSOL + TRADV) + DDAD + (THBU + THBA + 2THOTI + 2THOT + TCBU + TCBA) \quad (2)$$

Where:

At L2 we have: Probe (TPRB), Authentication (TAUTH), and Re-Association (TRASS) delays. For Route Discovery, we have: Router Solicitation (TRSOL) and Router Advertisement TRADV delays. Finally, BU and BAck delays with HA, 2THOTI, 2THOT: HoTi and HoT process and TCBU, TCBA: BU and BAck with CN.

e) Fast Handover Mobile Internet Protocol Version 6

FMIPv6 technology is designed to enhance the handover strategy in a MIPv6 network. The main here is to configure a new IP address or New Care-Of-Address (NCoA) or Previous CoA (PCoA) for the MN before it moves to the new network or new Access Router (AR). Specifically, FMIPv6 protocol enables a MN to request information about neighboring Access Points (APs) and the subnet information of AR's. In the FMIPv6 protocol, there are two types of handovers that have been identified, namely Predictive and Reactive handovers. In fact, MN will send a Router Solicitation for Proxy Advertisement (RtSolPr) message to the current AR requesting information for a potential handover. The AR will instantly reply with a Proxy Router Advertisement (PrRtAdv) message containing information about neighboring links. The PrRtAdv message also acts as a trigger for network-initiated handover. After the PrRtAdv message is received, the MN statelessly formulates a NCoA and sends a Fast Binding Update (FBU) to its PAR. Particularly, the FBU's aim is to bind the PCoA to the NCoA in order to tunnel the arriving packets to the new location of the MN. Afterwards, the PAR sends a Fast Binding Acknowledgement (FBAck) to the MN. This practically means that by the time the MN attaches to the NAR, the packet tunneling is already in progress. Fast Neighbour Advertisement (FNA) message will then be sent by the MN as soon as the MN is connected to the NAR. The FNA message is used not only to announce attachment between the MN and the NAR, but also to confirm the use of the NCoA [25] [26]. This scenario called the "predictive handover'' was used in this research materializing the host-based mobility approach used to enhance network performance of the proposed MIPv6-based client-server architecture.

III. Implementation

a) Methodology

This project implements a client-server architecture based on Mobile IPv6 and proposes technology upgrades to ensure server services continuity and node mobility management across different networks. Clients are provided seamless connection to server and services and with IPsec protocol implementation and Return Routability security procedure, network entities are provided a secure and trusted platform. Therefore, the proposed architecture as seen in Figure 2 was used to implement a client-server model based on MIPv6 using the discrete event simulator "OMNET++5.2" with INET Framework [27]. The simulation environment included different simulation packages and corroborated the technology used that improved MIPv6 operations basic principles by means of handover process, route optimization and tunneling

mechanism in the client-server environment. To implement FMIPv6, handover driven items were considered, developed and modified in OMNET++ based on specifications in [28] developed and standardized by the IETF Task Force under RFC 5568. So, all the modifications were brought up to adjust the handover impacting parameters to Fast Handover MIPv6 specifications, whilst all the implemented service model definitions in FTP, HTTP and Video Stream and configurations remained intact.

As a design research project, this study involved a comparative approach of two logically implemented technologies through simulation. Both MIPv6 and FMIPv6 in client-server were implemented with security and route optimization processes, which ultimately responded to the research objectives. The research included a dynamic data rate selection method based on IEEE 802.11g standard where bitrate automatically adjusts to lower rates to maintain connection and allow clients to communicate at the best possible speed. The standard includes 6, 9, 12, 18, 24, 36, 48, and 54 Mbps [29]. All three application services i.e. FTP, HTTP and Video Stream were configured using the dynamic bitrate approach and were used to implement the proposed client-server architecture using both TCP and UDP transmission protocols based on performance metrics such as handover latency, end-to-end delay, network throughput, packet loss rate (PLR), and Packet Error Rate (PER). However, Video Stream and FTP services were configured using a dynamic data rate selection mode (6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 32 Mbps, 48 Mbps and 54 Mbps) with different bitrates values that helped record and collect result on different simulation instances [30], whereas to test a single rate implementation, only HTTP was developed and configured with a unique bitrate value (54Mbps), all based on IEEE 802.11g.

After a successful MIPv6 implementation, FMIPv6 on the same network architecture to improve handover latency and service performance of the network with a faster handover process. Simulations instances could then be compared with respect to the implemented and tested application services. To analyze the collected data in result output, we used statistical quantitative data analysis approach employing the first order statistics such as average, or mean values that were displayed in the output results. Finally, the results obtained from the simulation were used to investigate different MIPv6 handover techniques' impact on the mobile and client-server network performance.

b) MIPv6 Client-Server Network Topology

The implementation of the network in Figure 2 was done in OMNET++ using INET. With one Home Network (HN), one Foreign Network (FN), one client and one server, the architecture illustrates the handover process, securtity through IPSec (using bidirectional packet tunneling method) protocol and Route Optimization process.

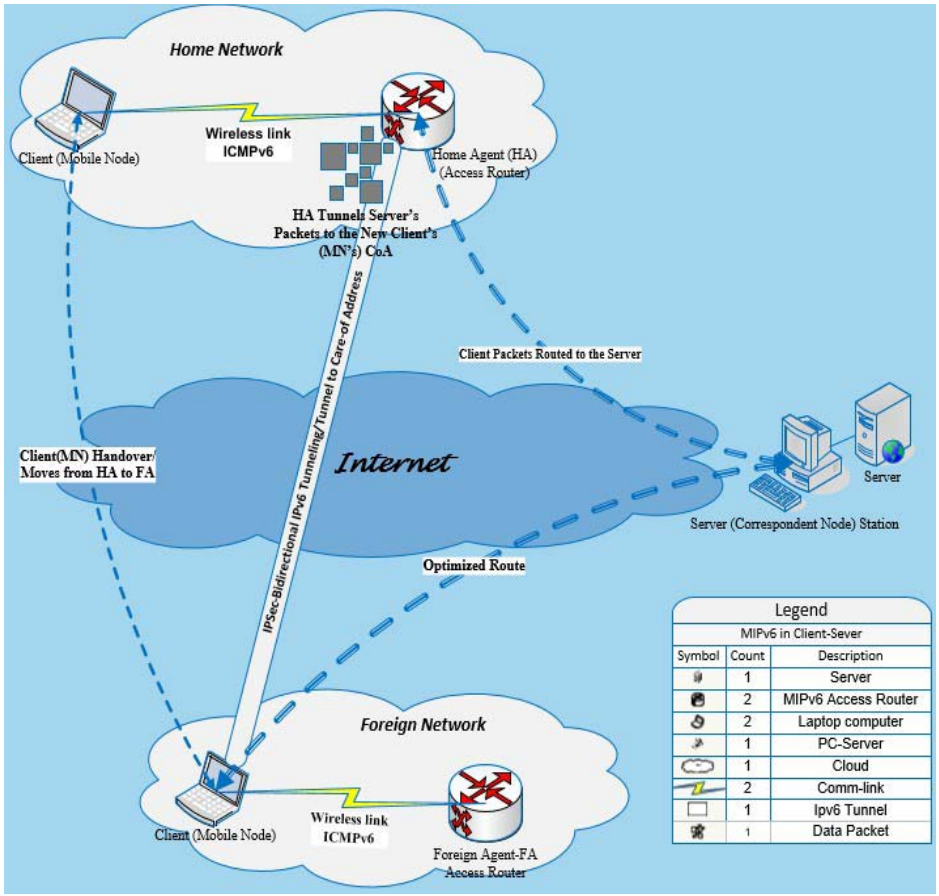

Figure 2: Proposed Topology of MIPv6 Network Simulation Model in Client-Server Environment

The MN or client was set to be moving across the sub networks without losing connection with the HA and the CN or server while keeping its original IP address for identification on internet. As the client moves from its HN to the FN, it establishes a bidirectional IPv6 communication tunnel with the HA to inform of its attachment to a different network by sending BU message carrying its CoA. At this point, for the packets to be routed between the server and the client, the HA is used to relay the two entities. But after a certain period of time, the client sends another BU message to the Server to establish a direct communication and start exchanging information without relying on the HA. The decision creates the Route Optimization process with extra security measure dependent of mobility extension headers in IPv6 that in carried out by RR procedure. So, until the client leaves the FN, it will be using the optimized route. Therefore, MIPv6 implementation included the development and configuration of handover related parameters that can be seen in Table 1.

Table 1: MIPv6 Initial Network Configuration Parameters

Attributes	*Values*
Simulation Time	120 Seconds
Num of Mobile Nodes	1
Number of Correspondent Nodes (Servers)	1
Neighbor Discovery Min Interval Between Ras	0.03s
Neighbor Discovery Max Interval Between RAS	0.07s
Wlan Management Authentication Steps	4
Wlan Bitrate	54 Mbps
Wlan Management Beacon Interval	0.1s
Wlan Agent Probe Delay	0.1s
Client Mobility Type	Rectangle Mobility
Client Mobility Speed	10mps

Furthermore, network traffic has been generated between the client and the server with three types of services HTTP, FTP and Video. Every service is defined with network characteristics and traffic model that runs between the client and the server as seen in Tables 2, 3 and 4.

Table 2: Traffic Model for Video Streaming

Application Traffic Model	Value
Simulation Time	120 Seconds
Start Time	3 Seconds
Server Port	3088
Video Size	25 Megabits
Send Message Interval	10 Milliseconds
Packet Length	1000 Bytes

Table 3: Traffic Model for Web Application

Application Traffic Model	Value
Simulation Time	120 Seconds
Start Time	4 Seconds
Server Port	80
Number of Req Per Session	1
Page Request maximum Size	Truncated in 350 Bytes and 20 Bytes

Table 4: Traffic Model for FTP Application

Application Traffic Model	Value
Simulation Time	120 Seconds
Service Start Time	3.5 Seconds
Server Port	21
File Size	20 Mega Bytes

c) *Proposed FMIPv6 Client-Server Network*

The overall concern in this project is how to avoid a longer handover latency and enable real-time applications such as video stream to be transmitted between the client and the server. Based on the technology standards and implementation procedures as standardized by IETF in RFC 5268 on mobile IPv6 fast handovers for 802.11 networks, the overall implementation could be carried out using test bed implementation, or a simulation that was performed in this research using OMNET++ [31].

At a higher degree, FMIPv6 and its functionalities relies on L2 triggers, hence on L2 handover, in order to execute L3 process in a faster way [32]. The aim of the technology is to allow an MN to quickly configure its NCoA before it moves and connects to a new network, and to use the NCoA immediately upon connecting to the new network (FA). So, FMIPv6 solution manages to reduce BU/Registration delay but in our research, we expanded the focus on the other three delay components including DL2, DRD, and DDAD.

- *Modifying L2 Delays:* In OMNET++, methods containing L2 triggers introduced in xMIPv6 were modified to obtain FMIPv6 in INET as needed. Furthermore, since the probing, or scanning delay is the most prevalent during an L2 handover, we believe that it merits special attention as affirmed in [33]. In fact, on its own, the probe delay maintains 90% of the total L2 handover delay [34].
- *Modifying Router Advertisements:* Router Solicitations (RSol) and Router Advertisement (RA) provide the MN with the necessary information for the creation of the NCoA to establish communication with the HA and the Server or CN. For better performance, networks require faster movement detection by modifying RAs values (MaxRtrAdvInterval and MinRtrAdvInterval). Therefore, we should necessarily allow a quicker sending of RAs more frequently than the 3 seconds establish in the standard MIPv6 [32]. In this project, we reduced RA intervals in an effort to deduce their effect on DRD delay.
- *Modifying Duplicate Address Detection (DAD):* one of the most effective metrics in affecting handover delay since the MN must bear a unique IP address while travelling across networks. In fact, it tries to find out if the given CoA address is unique or not in use by any other node in the network. In INET, the value emitted by this metric is of 1 second. To manage the fast handover implementation, we modified the emitted value in the source code by attributing 0 second to the DAD as noted in RFC 5568 and RFC 4862 [28].

IV. Results and Performance Evaluation

Considered as the most important applications of this study in terms of handover delay management, Video Stream's QoS performance measurements displayed on the graph in Figure 3 demonstrates how improved handover latency conditions in MIPv6 implementation may reduce the overall handover delay, therefore reducing network packet loss. However, as recorded, Throughput, Packet Loss Rate, Handover delay and End-to-End delay metrics were used to measure and evaluate the overall network performance of Video Stream services using UPD transmission, whilst via TCP protocol, network Throughput, and Packet Error Rate (PER) metrics were used to measure performance of FTP and HTTP network service performances. Network performance was tested and produced satisfying results for both MIPv6 and FMIPv6.

a) *Network Performance Evaluation with UDP Transmission*

i. *UDP Handover Delay for Video Stream Services*

Handover (HO) latency was then measure using UDP protocol with Video Stream services, the most

important application to be preserved in terms of packet loss as it requires a real-time format for the client to watch the stream at its best performance.

Figure 3 is a graph capturing handover delay values from the MIPv6 and FMIPv6 simulation instances, where we established the difference between the last time a packet was received by a client before the handover process and the next time the client receives a new packet after the handover process. The figure displays difference in handover delay between both MIPv6 and FMIPv6. This demonstrates that the maximum handover latency for MIPv6 network using UDP transmission is around 5 seconds, while it is reduced to 3.2 seconds in FMIPv6 implementation.

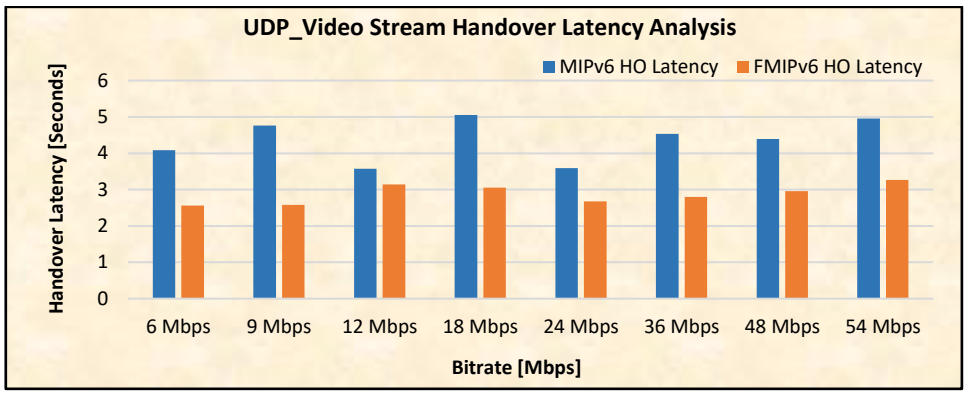

Figure 3: Handover Delay Results Report with UDP Protocol and Video Stream Service

ii. *UDP Packet End-To-End Delay for Video Stream Services*

Based on the Video Stream service configuration, packets transmitted between the client and the server introduced a very low end-to-end delay in the implementation of both MIPv6 and FMIPv6. Figure 4 shows steady decrease with a proportion of 0.6 milliseconds (ms) as the lowest value and 1.985 ms as the highest value for MIPv6, whilst Fast Handover MIPv6 process introduced a lower degree of delay in end-to-end communications between the client and the server with the lowest and the highest delays being of 0.5 ms and 1.903 ms, respectively.

Figure 4 demonstrates the difference in packet end-to-end delay between both the implemented MIPv6 and FMIPv6 with a clearly better network performance and ultimately better QoS since the handover latency is reduced.

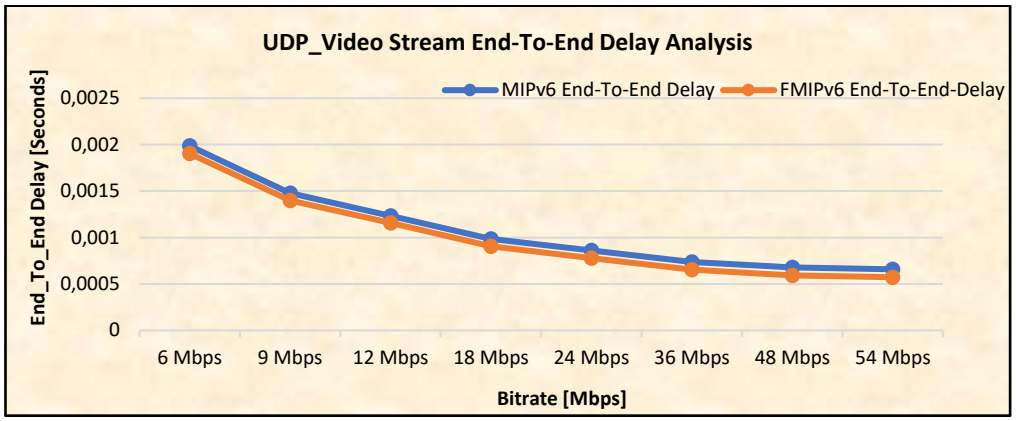

Figure 4: UDP End-To-End Delay for Video Stream

iii. *UDP Throughput for Video Stream Services*

As seen in Figure 5, the highest throughput performance in MIPv6 implementation was when the server was transmitting at 12 Mbps of bitrates with a relative value of 0.739 Mbps of throughput, while the lowest values was recorded at 18 Mbps with 0.729 Mbps of throughput performance. On the other hand, FMIPv6 technology bolstered the network throughput performance with at least 0.7406 Mbps as the lowest throughput value at bitrates of 54 Mbps, and 0.747 Mbps as the highest throughput value at 9 Mbps.

Figure 5 illustrates the overall performance evaluation results for QoS/Throughput metric with differences established between MIPv6 and FMIPv6 technologies implementation.

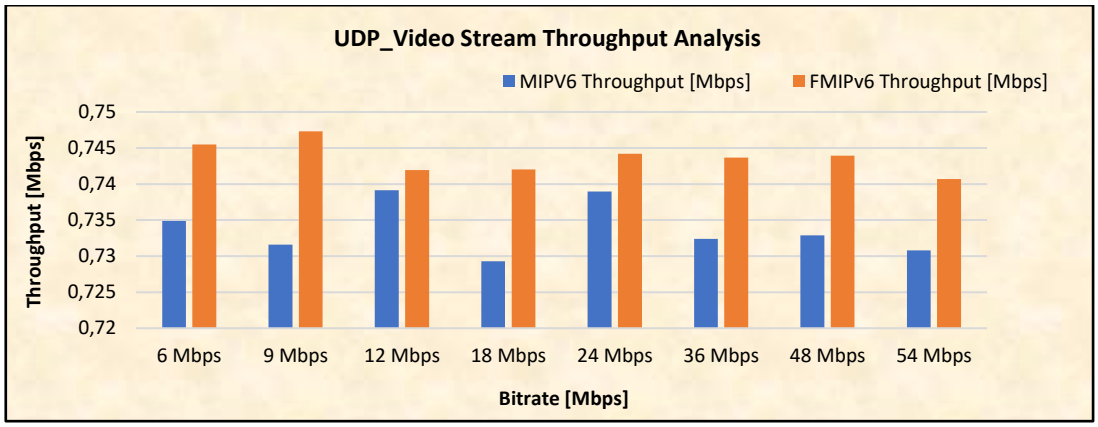

Figure 5: UDP Video Stream Throughput Implementation Results

iv. *UDP Packet Loss Rate for Video Stream Services*

Calculating the rate fell into seeking the percentage level of packet loss that the client encountered during the streaming of the video as opposed to what the server was transmitting in real-time (total number of packets sent). Thus, MIPv6 present its highest PLR at 18 Mbps with 6.5 % of sent packets lost, and the lowest at 12 Mbps with 5.2 %. On the other hand, the implementation of FMIPv6 expectedly decreased the loss rate value for all the tested bitrates values with the highest packet loss rate having been recorded at 54 Mbps with 5 % and the lowest PLR recorded at 9 Mbps with 4.1 %.

Figure 6 illustrates differences established between the total packets sent by the server and those received by the client, and then calculated the percentage of the number based on the total packets sent by the server.

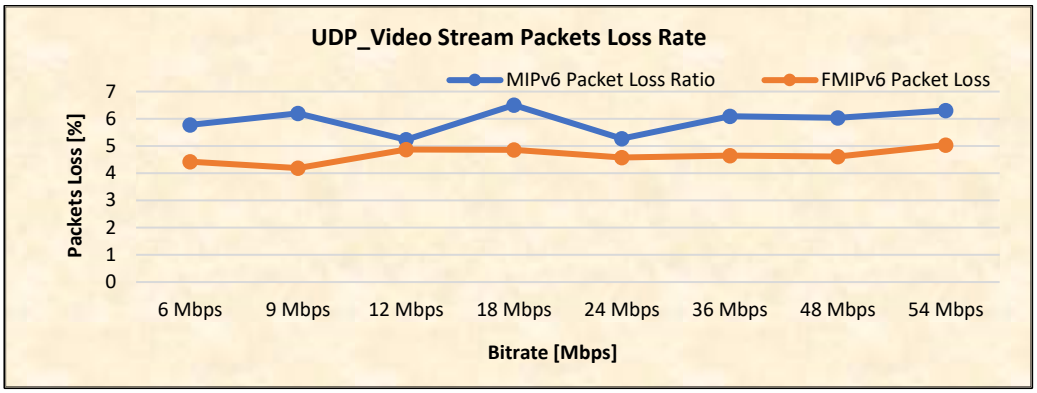

Figure 6: UDP Video Stream Packet Loss Rate Implementation Results

b) Network Performance Evaluation Using TCP Transmission

i. *TCP Network Throughput for File Transfer Protocol Services*

The results in Figure7 show that the lowest value of the overall TCP throughput implementation for MIPv6 was 53.5 Kbps recorded at 12 Mbps, and the highest valued being of 81.47 Kbps was recorded at 48 Mbps. On the other hand, FMIPv6 displayed a starling increase in some instances while in others the gap was of a narrowed proportion. Thus, for Fast Handover MIPv6 the highest displayed throughput was of 111.29 Kbps recorded at 54 Mbps, and the lowest value being of 59.74 Kbps was recorded at 9 Mbps.

Figure 7presents the overall throughput performance in terms of network QoS for both MIPv6 and FMIPv6 establishing differences based on configured bitrates values. Throughput for this service is measured in Kbps.

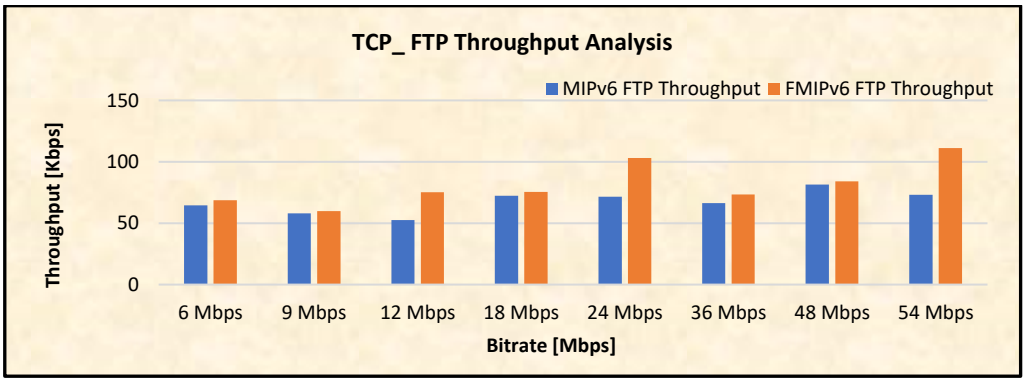

Figure 7: TCP FTP Throughput Implementation Results

ii. *TCP Packet Error Rate for File Transfer Protocol Services*

As suggested by [35], Packet Error Rate as a metric is very critical to connection-oriented communications. Therefore, the implementation of MIPv6 as well as the enhanced FMIPv6 demonstrated the sensitivity of TCP (with FTP service here) protocol in terms of PER as shown in Figure 8, since both technologies recorded 0 % of loss in packets for almost all the bitrates values. However, even though some values were recorded for both 48 Mbps with and 54 Mbps in packet error rate estimates, they were of a very insignificant (very close to 0%) proportion, responding to the sensitivity of TCP communications to errors in packets.

Figure 8 illustrates the fundamental issue of packet error rate (PER) in File Transfer Protocol service implementation with significantly negligible values which appeared appropriately respondent to the exigence of TCP protocol.

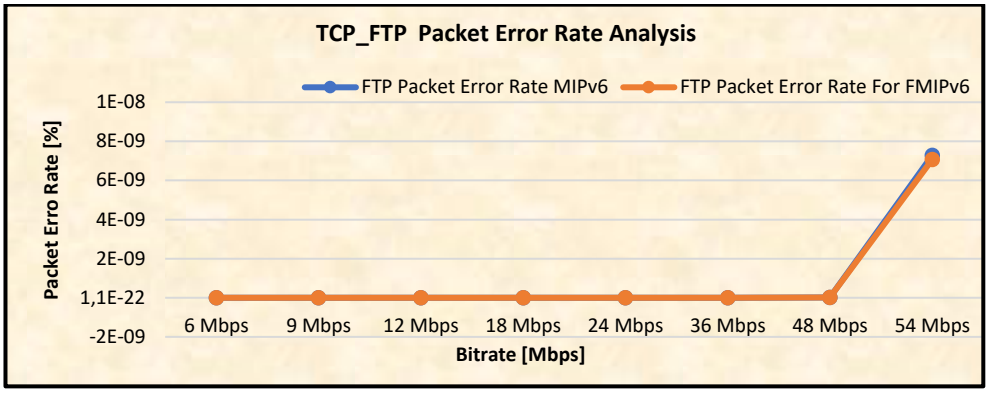

Figure 8: TCP FTP Packet Error Rate Implementation Results

iii. *TCP Throughput for HTTP Services*

Figure 9 shows the results, where in MIPv6 implementation, the network throughput value was of 418.05 Kbps, whilst it was up to 520.678 Kbps for FMIPv6, highlighting the importance of handover latency improvement driven techniques in MIPv6 network experiences.

Figure 9 shows the throughput implementation results for HTTP services over TCP protocol as we opted to consider only one instance of bitrate for both MIPv6 and FMIPv6 in client-server network.

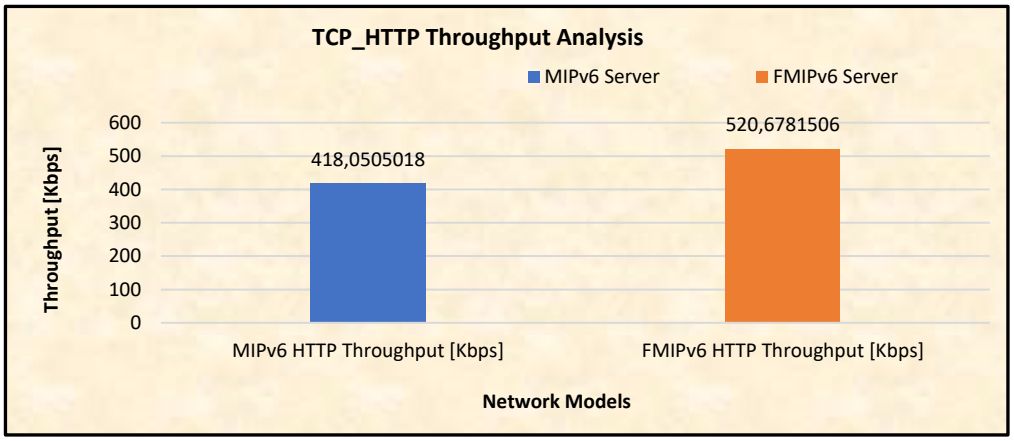

Figure 9: TCP HTTP Throughput Implementation Results

iv. *TCP Packet Error Rate for HTTP Services*

Based on a single bitrates value (54 Mbps) for both MIPv6 and FMIPv6 client-server implementation, and with a less significant difference, Fast Handover MIPv6 outperformed the standard MIPv6 with recorded PER of 0 %, while PER for MIPv6 in HTTP services implementation was very low (close to 0 %), reiterating the consistency of a low or inexistent PER for TCP-related services.

Figure 10 illustrates the Packet Error Rate implementation results for HTTP services over TCP transport protocol considering one bitrate instance (54 Mbps) as configured in the general simulation configuration that we set up for both MIPv6 and FMIPv6 network simulation instances in Table 1.

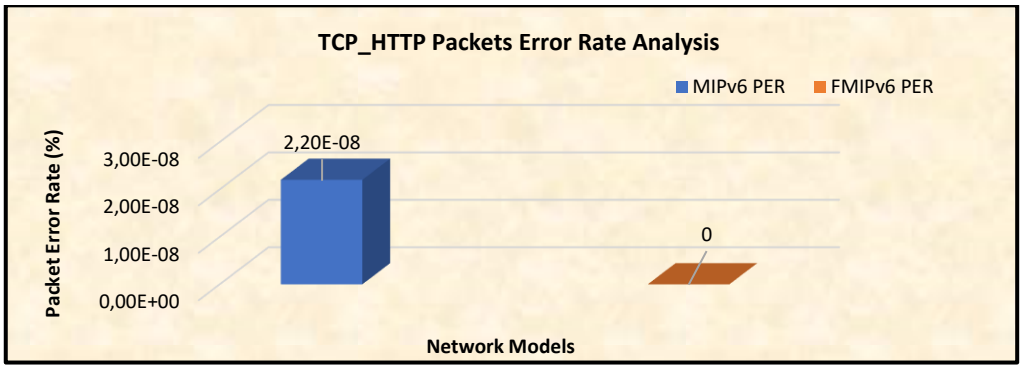

Figure 10: TCP HTTP Packet Error Rate Implementation Results

V. Discussion and Conclusion

All the objectives in this research have been met. Indeed, for specific objective 1, literature was obtained, analyzed and applied to different study areas. It gave insights on MIPv6 and related areas and on the prospect of their interaction with client-server technology to attain the purpose of the project. Based on the literature, this objective allowed the determination of a more optimized and secure way of communication in MIPv6 based networks to ensure security and better network performance. The proposed techniques included a bidirectional tunneling through IPSec and Route Optimization. Through specific objective 2, which aimed to design and implement the proposed network architecture, the research produced a technical and architecture commodity that implemented MIPv6 and FMIPv6 technologies (through simulation) in client-server architectures with respect to important technical requirements such as security and Route Optimization. Since MIPv6 was poised to introduce a rather longer handover delay, which was deemed unsatisfactory to real-time applications and the needed better network performance, specific objective 3 has been met, since the implementation was able to evaluate network performance of MIPv6 technology in client-server architecture and ensured a decrease in handover latency by introducing another handover technology approach, FMIPv6. The architecture was implemented based on different application service models as shown in Tables 2, 3 and 4. MIPv6 solution provided technological abilities to a client-server technology where it becomes possible to seamlessly manage connection with clients as they move and attach to other IPv6-based networks in foreign environments. However, as illustrated in Table 5, handover delay time in MIPv6 is still critical for real-time application and for the overall network performance. Therefore, the implementation of

FMIPv6 on the same architectural dispositions improved handover latency and provided a better performance to the network.

Table illustrates handover delay measurements between MIPv6 and FMIPv6 using UDP transmission based on Video Stream Application. The table show the highest handover delays difference between MIPv6 and FMIPv6 implementation instances. For MIPv6 the highest delay was recorded at 18 Mbps whist for FMPv6 the highest was recorded at 12 Mbps as shown in Figure 3. So, the maximum handover time of MIPv6 is 5 seconds and FMIPv6 is approximately 3 seconds resulting in a significantly lower latency time in the network.

Table 5: Total Handover Time MIPv6/FMIPv6 implementation instances

Technology	*Transmission Bitrate in Mbps*	*Highest Handover Delay in Seconds*
MIPv6	18	5.05
	12	3.59
FMIPv6	18	3.05
	12	3.14

Furthermore, we can see that the overall network performance was practically improved with FMIPv6 implementation based on all the measurement metrics used in this research. Remarkably, throughput in both MIPv6 and FMIPv6 is performing poorly for TCP implementation than for UDP implementation as seen in Figures 5, 7 and 9. However, FMIPv6 always produces a better performance perspective than MIPv6 for the throughput analysis. The UDP End-To- End Delay for both MIPv6 and FMIPv6 was remarkably low with a steady decrease in value as bitrates values increase as shown in Figure 4. Figure 6 shows a critical Packet Loss Rate in UDP Video Stream implementation for MIPv6 that was improved in FMIPv6 implementation, while TCP Packet Error Rate was close to and equal to 0% for MIPv6 and FMIPv6 respective implementations as shown in Figures 8 and 10. Finally, the research concluded that implementing client-server networks based on MIPv6 technology enhanced network capacity and expanded ability of communication between clients and servers with a seamless and roaming communication capability and service handover of nodes in mobility to different networks. However, the overall network performance and QoS was rendered better in improving the network handover delay by implementing FMIPv6 in extension of MIPv6 for FTP, HTTP and Video stream services. Finally, the most important recommendation for future work is that there should be considered more than one Home Agent. This may increase security and service availability issues in case of disaster occurrence since one HA represents a single point of failures. So, more HA can possibly be securely added and synchronized with the MN to increase availability posture and prevent fatal security breaches.

References Références Referencias

1. S. Céspedes and S. Sherman, "On Achieving Seamless IP Communications in Heterogeneous Vehicular Networks," vol. 16, pp. 1–15, 2015.
2. N. Zhang and H. Bao, "Study on Mobile IP Technology in Wireless Communication Systems," in ICWMMN200B Proceedings, 2008, pp. 1–4.
3. D. Ma and M. Ma, "Network selection and resource allocation for multicast in HetNets," Journal of Network and Computer Applications, vol. 43, pp. 17–26, 2014.
4. W. Goralski, "Learn About Differences in Addressing Between IPv4 and IPv6," Juniper Networks, pp. 1–11, 2014.
5. S. Kim and D. Y. Kim, "Home Address allocation to mobile terminal over mobile IP environments," no. 0, 2006.
6. M. Laurent-Maknavicius, "For a Secure Mobile IP and Mobile IPv6 Deployment," no. section 6, pp. 109–120, 2002.
7. Z. S. Fei, C. W. Xing, and N. Li, "QoE-driven resource allocation for mobile IP services in wireless network," Science China Information Sciences, vol. 58, no. 1, pp. 1–10, 2014.
8. S. K. Opoku, "A Simultaneous-Movement Mobile Multiplayer Game Design Based on Adaptive Background Partitioning Technique," pp. 2–4, 2012.
9. C. Perkins, D. Johnson, and J. Arkko, "Mobility Support in IPv6," 2011.
10. S. Glass, T. Hiller, S. Jacobs, and C. Perkins, "Mobile IP Authentication, Authorization, and Accounting Requirements," no. October, pp. 1–27, 2000.
11. P. Lin, S. M. Cheng, and W. Liao, "Modeling key caching for mobile IP authentication, authorization, and accounting (AAA) services," IEEE Transactions on Vehicular Technology, vol. 58, no. 7, pp. 1–3, 2009.
12. G. Yang, Z. Lei, H. Wang, Y. Dou, and Y. Xie, "Analysis of the RADIUS signalling based on CDMA mobile network," Proceedings - 2014 6th International Conference on Intelligent Human-Machine Systems and Cybernetics, IHMSC 2014, vol. 2, pp. 270–274, 2014.

13. C. E. Perkins, "Mobile IP and the IETF Mobile Networking at IETF 45," vol. 3, no. 3, pp. 4–7, 2002.
14. G. Bai and C. Williamson, "The effects of mobility on wireless media streaming performance," Proceedings of Wireless Networks and Emerging Technologies (WNET), pp. 596–601, 2004.
15. F. Xiaorong, L. Jun, and J. Shizhun, "The research on mobile Ipv6 security features," IEEE Symposium on Wireless Technology and Applications, ISWTA, pp. 125–128, 2013.
16. V. Heydari, S. Kim, and S.-M. Yoo, "Secure VPN using Mobile IPv6 based Moving Target," EEE, pp. 7:1-7:8, 2016.
17. D. Rudolf, "Next Generation Internet : IPv4 Address Exhaustion, Mitigation Strategies and Implications for the U.S," Ieee Usa, pp. 1–26, 2009.
18. O. Babatunde and O. Al-debagy, "A Comparative Review of Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6)," International Journal of Computer Trends and Tecnology, vol. 13, no. 1, pp. 10– 13, 2014.
19. J. Hyun, J. Li, H. Kim, J. H. Yoo, and J. W. K. Hong, "IPv4 and IPv6 performance comparison in IPv6 LTE network," 17th Asia-Pacific Network Operations and Management Symposium: Managing a Very Connected World, APNOMS 2015, pp. 1–6, 2015.
20. T. Sanguankotchakorn and P. Jaiton, "Effect of triangular routing in mixed IPv4/IPv6 networks," Proceedings - 7th International Conference on Networking, ICN 2008, no. May 2008, pp. 357–362, 2008.
21. H. R. Hamandi and D. E. H. Al-Hemiary, "Simulation of Mobile IPv6 Using OMNeT ++ Simulator," vol. 13, no. 1, pp. 49–54, 2013.
22. S. J. Vaughan-Nichols, "Mobile IPv6 and the future of wireless internet access," Computer, vol. 36, no. 2, pp. 18–20, 2003.
23. B. M. Al-Kasasbeh, R. E. Al-Qutaish, and K. T. Al-Sarayreh, "Indirect Routing of Mobile IP : A Non-Encapsulation Approach," International Journal of Computer Science and Network Security, vol. 8, no. 7, pp. 124–131, 2008.
24. R. Radhakrishnan, M. Jamil, and S. Mehfuz, "A Robust Return Routability Procedure for Mobile IPv6," vol. 8, no. 5, pp. 234–240, 2008.
25. M. A. Amin, K. B. A. Bakar, A. H. Abdullah, and R. H. Khokhar, "Reducing handover latency in mobile IPv6- based WLAN by parallel signal execution at layer 2 and layer 3," Communications in Computer and Information Science, vol. 154 CCIS, pp. 201–211, 2011.
26. D. Phoomikiattisak and S. N. Bhatti, "Mobility as a first class function," 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob 2015, pp. 850–859, 2015.
27. A. Al-Rubaye, A. Aguirre, and J. Seitz, "Enabling Soft Vertical Handover for MIPv6 in OMNeT++," 2016.
28. R. Koodli, "Mobile IPv6 Fast Handovers," 2009.
29. S. Sendra, M. Garcia, C. Turro, and J. Lloret, "Wlan Ieee 802.11 a/B/G/N Indoor Coverage and Interference Performance Study," International Journal on Advances in Networks and Services, vol. 4, no. 1, pp. 209–222, 2011.
30. F. Tramarin, S. Vitturi, and M. Luvisotto, "A dynamic rate selection algorithm for IEEE 802.11 industrial wireless LAN," IEEE Transactions on Industrial Informatics, vol. 13, no. 2, pp. 846–855, 2017.
31. R. Koodli, "Mobile IPv6 Fast Handovers," 2010.
32. V. Vassiliou and Z. Zinonos, "An Analysis of the Handover Latency Components in Mobile IPv6," Journal of Internet Engineering, pp. 230–240, 2010.
33. J. Lai, Y. A. Sekercioglu, N. Jordan, and A. Pitsillides, "Performance Evaluation of Mobile IPv6 Handover Extensions in an IEEE 802. 11b," vol. 6, pp. 1–8, 2006.
34. M. Zaidi, J. Bhar, R. Ouni, and R. Tourki, "Reducing Wi-Fi handover delay using a new positioning process," in 2011 International Conference on Communications, Computing and Control Applications, CCCA 2011, 2011, no. January.
35. S. Abukharis, J. A. Alzubi, O. A. Alzubi, and S. Alamri, "Packet error rate performance of IEEE802.11g under bluetooth interface," Research Journal of Applied Sciences, Engineering and Technology, vol. 8, no. 12, pp. 1419–1423, 2014.