Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI:10.21474/IJAR01/16272
DOI URL: http://dx.doi.org/10.21474/IJAR01/16272

RESEARCH ARTICLE

MOBILITY MANAGEMENT IN A CROSS-DOMAIN SDN ARCHITECTURE LEVERAGING THE IPV6 MOBILE PROXY

Akichy Adon Jean Rodrigue Kanda[1], Amanvon Ferdinand Atta[2], Michel Babri[1] and Ahmed Dooguy Kora[3]

1. Laboratoire de Recherche en Informatique et Télécommunication, Institut National Polytechnique Félix Houphouët-Boigny, Yamoussoukro, Côte d'Ivoire.
2. Unité de Recherche et d'Expertise Numérique, Université Virtuelle de Côte d'Ivoire, Abidjan, Côte d'Ivoire
3. Ecole Supérieure Polytechnique, Université Cheikh Anta Diop, Dakar, Sénégal.

Manuscript Info

Manuscript History
Received: 15 December 2022
Final Accepted: 19 January 2023
Published: February 2023

Key words:-
IP Mobility, Software Defined Networking (SDN), Handover, Proxy Mobile IPv6 (PMIPv6)

Abstract

Mobility and technology have become inseparable terms in the sense that users want to stay connected and continue to use their services while moving. The various technologies that manage mobility face fundamental challenges such as optimizing intra-domain and inter-domain routes.With the emergence of Software-Defined Networking (SDN), a promising technology that separates the control plane from the data plane in network devices, mobility management could benefit from its advantages and thus address the above challenges. In this paper, we propose a new method of communication during the movement of a mobile node between two different domains based on the operation of the PMIPv6 protocol in a software defined networking (SDN) architecture and the involvement of edge nodes to anticipate the new destination of the mobile node. The proposed method is inspired by proactive and reactive inter-domain handovers and allows the controller to anticipate inter-domain communication with its peers and simultaneously reduce the handover time in the visited domain and the data transfer delay. The experimental results confirmed the effectiveness of the proposed method.

Introduction:-

With technological progress, we are witnessing an exponential growth in network traffic due to the abuse of mobile devices that access the internet and can use all types of network services as users can stay connected anywhere and at any time[1]. Managing consumer mobility to ensure session and service continuity in an efficient and effective manner is becoming increasingly challenging owing to the increasing number of mobile devices and their high mobility patterns. Thus, mobility management is becoming an essential domain to develop to ensure a good user experience.

However, the current architecture used by Internet Protocol(IP) does not facilitate mobility management. Indeed, the Internet is dominated by the client/server mode, which means that a logical connection between a client and a server is based on a socket composed of IP addresses, port numbers of the two terminals and a protocol[2]. The connection must be re-established if any of these parameters are changed. In a mobile environment, the IP address and port number of a client change, as soon as it connects to another gateway. The client re-establishes a logical connection

Corresponding Author:- Akichy Adon Jean Rodrigue Kanda
Address:- Laboratoire de Recherche en Informatique et Télécommunication, Institut National Polytechnique Félix Houphouët-Boigny, Yamoussoukro, Côte d'Ivoire.

with the server by using the new IP address. This interruption of the connection causes delays and degradation of service and user experience.

To address these challenges, research in this area has focused on different IP mobility management protocols (Mobile IP and its derivatives)[3]. Mobility management protocols fall into two main groups, network-based and host-based protocols.

However, when mobility involves frequent interface changes, network-based mobility management protocols seem more suitable. Indeed, the mobile host can maintain its IP address while moving, unlike other mobility protocols where mobility management requires tracking the host's movements and initiating the required mobility signaling on its behalf[4].

This paper based on the SDN concept leverages the Mobile IPv6 Proxy Protocol (PMIPv6) by leveraging the strategic position of edge nodes in managing inter-domain communications. This new approach allows us to anticipate the new destination of the mobile device to react proactively and reduce the delay of the mobile device in the visited domain thus reducing the IP handover delay.

The remainder of this paper is organized as follows: Section II presents existing solutions for mobility management in IPv4, IPv6, SDN networks and their limitations. Section III provides further details regarding the proposed method. Section IV focuses onthe simulations and results. Finally, we conclude the paper with a summary of our work and perspectives.

Related works

Mobile IP technology

Many studies have been conducted to provide continuous and ubiquitous Internet services. Several solutions to support mobility have been proposed by the Internet Engineering Task Force (IETF) at the network layer. Among these solutions, there are the Mobile IP technologies (MIPv4, MIPv6) and their extensions.

Before going into detail, it is worth setting the context for the discussion by establishing terminologies, adapted from the Mobile IP specification. Mobile IP introduces the following new functional entities.

1. Mobile Node (MN): A host or router with the ability to change its home base from one network or subnet to another. A mobile node can continue to communicate with other Internet nodes at any location by using its (constant) IP address.
2. Home agent: A router in the home network that is responsible for delivering datagrams to mobile nodes.
3. Foreign agent: A router that belongs to the network visited by the mobile node.
4. Mobile Access Gateway: a router responsible for controlling the signaling of the mobile node.
5. Mobility anchor: an origin agent that tracks the movement and maintains the up-to-date location information of the mobile node in a MIPv6 domain.

A mobile node can have several addresses simultaneously. Mobile IP is a means of performing three related functions: the mobile node acquires an IP address in its parent network when it first connects, which is called the primary address. This address will always be used by the mobile node and its correspondents to identify communications at the application level. Indeed, if all correspondents had to be told the new address of the mobile node each time they moved, communication would have to be reinitialized each time. Therefore, communication is broken every time a mobile node moves, which is inefficient. Therefore, it is the main address that correspondents use as their destination address, regardless of the position of the mobile node. In addition, the mobile node may hold temporary addresses, known as temporary addresses. This address is obtained by the mobile node each time it enters a visited network. The mobile node will have to indicate this address to its home agent (and possibly to its correspondents in MIPv6) periodically so that it can maintain correspondence between the main and temporary addresses.

The 802.11 standard

802.11 is the most widely deployed wireless LAN standard. It covers the first two layers of the OSI model, the physical layer, and the medium access control (MAC) layer. An 802.11 LAN is based on cellular architecture (the system is subdivided into cells), where each cell (called a Basic Service Set, BSS in 802.11 nomenclature), is controlled by an Access Point (called an Access Point thus playing the role of a Base Station) [5]. All access points are interconnected by a backbone (called a Distribution System or DS). IEEE 802.11 networks can be configured in two modes: infrastructure and Ad-Hoc. The Ad-hoc mode allows direct communication between terminals without the intervention of central infrastructure. However, in infrastructure mode, an access point is required to connect all stations to the distribution system (DS) and thus all terminals communicate through this access point[3]. This is often called hybrid architecture. This mode was used in this study (see section xxx) article. The original IEEE 802.11 standard was published by the 802.11 group in its initial version allowing data to be transmitted in the 2.4 GHz ISM (Industrial Scientific Medical) band at a rate of 2 Mbps [5]. To improve this standard, other versions were released by the 802.11 group. The IEEE 802.11b standard allows a data rate of 11 Mbps to be achieved in the ISM band using the Direct Sequence Spread Spectrum (DSSS) modulation technique [6].

This standard although preferred for most mobile terminals, suffers from high latency when the mobile terminal is in motion, which is due to the distance between the mobile and the access point, or interference because of multiple mobiles in the same domain and mainly due to searching for a new access point because of the movement of the mobile. In the remainder of this section, we discuss mobile technologies that have emerged to address these issues.

Existing mobility approaches

Solutions based only on mobility management protocols.

Mobile IPv4 (MIPv4)[7]is the oldest mobility management technique for IP. Its success is attributed to its simplicity and flexibility. It has been the basis of several IETF documents [8]. IP mobility management consists of locating and routing IP packets to the mobile node. The mobile node has a reference network and a reference address in that network. This address always identifies the mobile node.

Mobile IPv6 (MIPv6) [6][7]is an upgrade of the IP protocol that uses the mechanisms of the MIPv4 protocol and adds several additional features. It is a widely accepted proposal for providing global mobility to mobile nodes. However, MIPv6 suffers from significant signaling overhead and long transfer delay. The IETF has standardized some extensions to MIPv6 to improve transfer performance. For example, PMIPv6 requires network entities to manage a mobility management process [9], [10], and exempts MNs from mobility signaling. In Fast Forwarding for PMIPv6 (PFMIPv6) [11], a bi-directional tunnel between the previous and next attachment points is established to eliminate packet loss by exchanging signaling messages [12].

In PMIPv6 solutions, when a mobile node enters a PMIPv6 domain for the first time, it must register with the anchor. This control signaling is performed by a Mobile Access Gateway (MAG) on behalf of the mobile node. Once the layer-two connectivity is complete, the mobile node sends a Router Request (RR) message to the gateway [9]. Upon receiving the RS message, the gateway sends the mobile node ID to an Authentication, Authorization and Accounting server (AAA server) for authentication. In response, the AAA server authenticates the mobile node and provides the gateway with the Home Network Prefix (HNP) of the mobile node. The gateway then sends a Proxy Binding Update (PBU) message to the anchor, which contains the mobile node ID and HNP. The anchor creates and updates an IP tunnel with the gateway and makes the appropriate entries in its routing table before responding with a Proxy Link Acknowledgement (PBA) message. When the gateway receives the acknowledgement, it makes an entry in the routing table and creates/updates the IP tunnel with the anchor. This establishes a bi-directional IP tunnel between the gateway and the anchor for data communication. The gateway sends a Router Advertisement (RA) message to the mobile node via the anchor before the data flow starts between the mobile node and the corresponding node.

In the case of handover, a mobile node disconnects from its previous gateway (pMAG) and sends an RS message to the next gateway (nMAG). The remainder of the control signaling is similar to the registration process of a mobile node. The correspondent node is unaware of the mobile node's handover, as the anchor makes the necessary changes to its routing table and routes the data packets received from the correspondent node over the new IP tunnel created with the next gateway while retaining the IP address of the mobile node. The control signaling involved in the forwarding procedure increases the time during which the mobile node is disconnected, resulting in packet loss, which is unacceptable for real-time services. Our design of the NO-PMIPv6 architecture is motivated by low handover latency, reduced packet loss, compatibility with existing PMIPv6 and scalability. The proactive scheme of the proposed architecture should achieve handover latency and packet loss within an acceptable range for real-time services, while avoiding overloading the gateways and the anchor with extensive control signaling and leveraging the strategic position of the domain edge nodes.

MIPv6-based protocols are centralized mobility management solutions, i.e., they leverage a central node called a mobility anchor that handles both mobile node location tracking and traffic redirection. This places a heavy load on the mobility anchor and negatively affects network quality. [13]

To avoid these limitations, solutions based on certain nodes of the network to free the load of the anchor and to allow fluidity of the traffic have emerged, such as distributed mobility management solutions and those based on the paradigm of software defined network.[13], [14]

Software Defined Networking Solutions.

In [15], an OpenFlow enabled mobile IPv6 proxy (OF-PMIPv6) was proposed, which separates the control path from the data path. Specifically, the mobility control function resides in the controller, whereas the data paths between the MAGs and MA are maintained as an IP data tunnel. In[16], a DMM scheme (S-DMM) was proposed based on SDN architecture. The S-DMM removes mobility logic from access routers and provides flow-based mobility support. S-DMM achieves a forwarding performance similar to that of the existing DMM but facilitates mobility management. In [17], an OpenFlow-based Mobile IPv6 Proxy (OPMIPv6) was proposed using the advantages of the OpenFlow architecture. In OPMIPv6, the LMA functions reside in an SDN controller, but the MAG function is implemented either in an access switch or in the controller. It mitigates the IP-in-IP tunneling overhead using OpenFlow flow table-based routing. In [18], a DMM solution (SDN-DMM) was proposed based on SDN architecture. In the SDN-DMM, mobility control is implemented as an application in the controller, which allows the advantages of the SDN architecture to be used. In [18], a distributed IP mobility management scheme was presented by adopting the SDN technology. This scheme is a flat mobile network architecture that eliminates a single failure point. In addition, it uses multiple controllers to harmonize the distributed mobility management mechanisms and so that there is no master controller. The aforementioned SDN-based solutions can facilitate mobility management by exploiting the advantages of SDN. In [19] a solution based on PMIPv6 and SDN introduced additional control signaling in OF-PMIPv6. The reactive and proactive forwarding schemes of this solution allow an improvement in terms of forwarding latency and packet loss compared to standard PMIPv6.

Proposed Method:-

This study proposes a NO-PMIPv6 method that leverages an architecture as shown in Figure 1, based on the OpenFlow protocol and PMIPv6.The Mobile Nodes (MNs) connect to OpenFlow-enabled edge switches via single-hop wireless communication. An MN is initially attached to a Mobile Access Gateway (MAG) and can establish multiple end-to-end flows with fixed correspondent nodes (CNs) in the wired network or mobile CNs in the wireless network. When a MN moves from the original mobile access gateway (OMAG: Original Mobile Access Gateway) to a new gateway (NMAG:New Mobile Access Gateway) in the same SDN domain, an intra-domain handover is triggered. Otherwise, an inter-domain handover occurs when the MN moves to a new gateway in another SDN domain.

In the following, we describe the connection steps in PMIPv6 followed by our proposal

First connection

Step1:When a MN moves into the coverage area of an Access Point (AP) and attempts to establish an end-to-end flow, it starts the registration process to obtain an IPv6 address. It first sends a Router Request (RS) message to the OMAG to apply a Home Network Prefix (HNP). The OMAG receives the RS message, which carries the MN identifier, and in turn sends this message to the domain controller as it has no rules for handling this message. In turn, the controller authenticates and updates the routing table with a Proxy Binding Update (PBU) message which includes its routable address.

Step 2: the MN identifier generated by the mobility anchor (LMA) is sent to the controller then routed to the OMAG. A bi-directional IP data tunnel was created between the anchor and OMAG for the transmission of data packets.

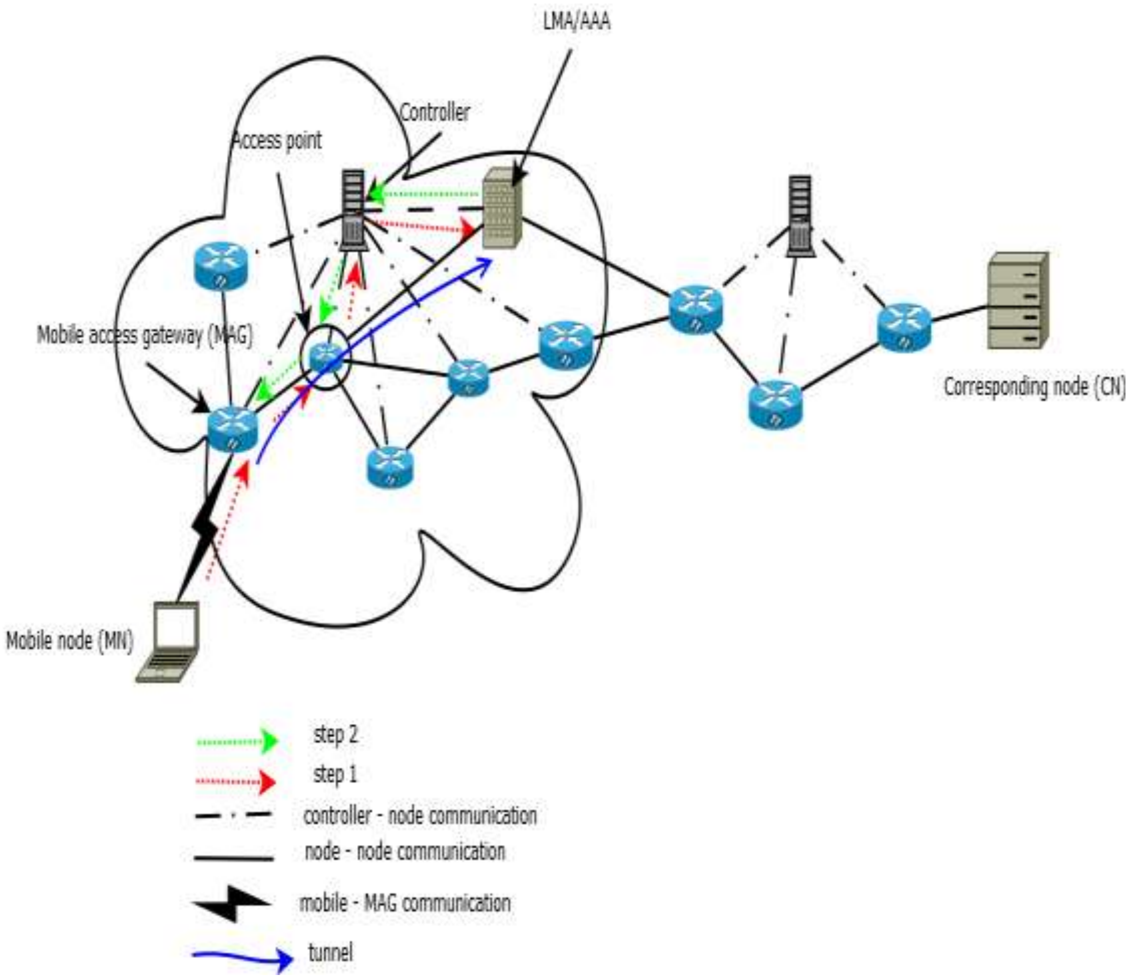
LMA/AAA
Controller
Access point
Mobile access gateway (MAG)
Corresponding node (CN)
Mobile node (MN)
step 2
step 1
controller - node communication
node - node communication
mobile - MAG communication
tunnel

Figure 1:-Scheme 1 NO-PMIPv6.

Management of inter-domain transfer

Step 1:When a MN leaves its domain, it triggers an inter-domain handover process. In NO-PMIPv6, for each edge node EN belonging to the current domain of MN,

Step 2: The controller computes the shortest distance between EN and MN. Thus, when the MNis close to a domain boundary, the distance between MN and the edge node of that boundary tends to 0. A proactive mechanism was triggered when this distance is equal to 1.

Step 3: There is an election of candidate domains and then the transfer of the mobile node's information to the elected domain controller so that the mobile node is taken care of without delay upon its arrival.

Step 4: Indeed, SDN controllers can communicate with each other through the West/East interface [10], which supports the exchange of mobility-related signals between different domains, and thus global mobility is achieved in

Step 4: Indeed, SDN controllers can communicate with each other through the West/East interface [10], which supports the exchange of mobility-related signals between different domains, and thus global mobility is achieved in the proposed scheme.

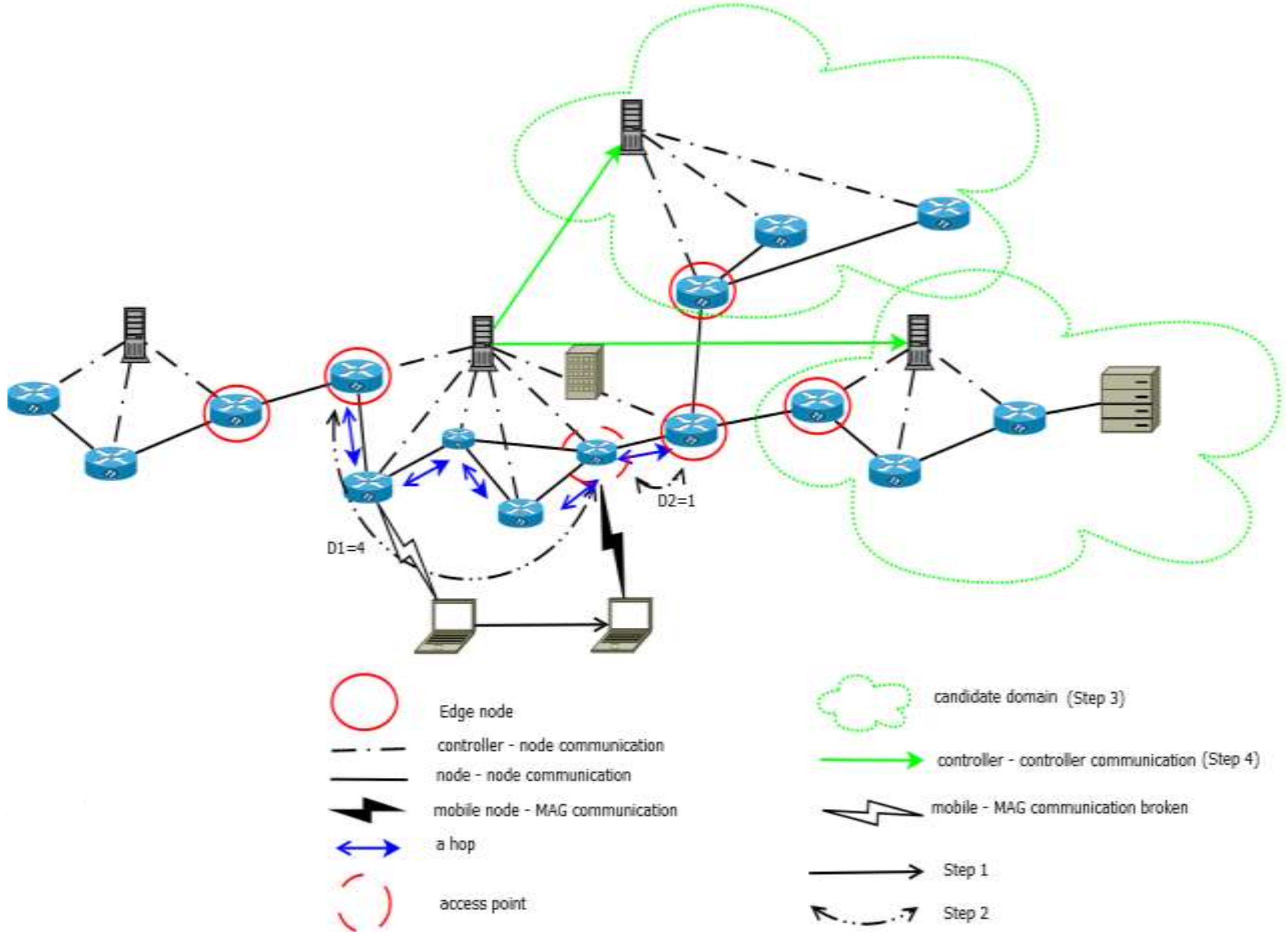
D1=4
D2=1
Edge node
controller - node communication
node - node communication
mobile node - MAG communication
a hop
access point
candidate domain (Step 3)
controller - controller communication (Step 4)
mobile - MAG communication broken
Step 1
Step 2

Figure2:-Scheme 2 NO-PMIPv6.

Analytical model

This section presents the analytical model of the proposed NO-PMIPv6 solution. In this study, the mobile node handover delay corresponds to the handover latency and is defined as the time interval during which a MN cannot receive any data packet while it is moving. The notations used in our analysis are summarized in Table 1 with their definitions.

Table 1:- definition of delay parameters.

D	Registration process time frame
T_{WRS}	delay between the establishment of the connection to the home point and the sending of the first packet
T_A	is the time needed to authenticate the mobile node to the AAA server
T_{PU}	time taken by PBU and PBA messages
T_R	wireless channel propagation delay and service delay at the gateway

Standard mobility management

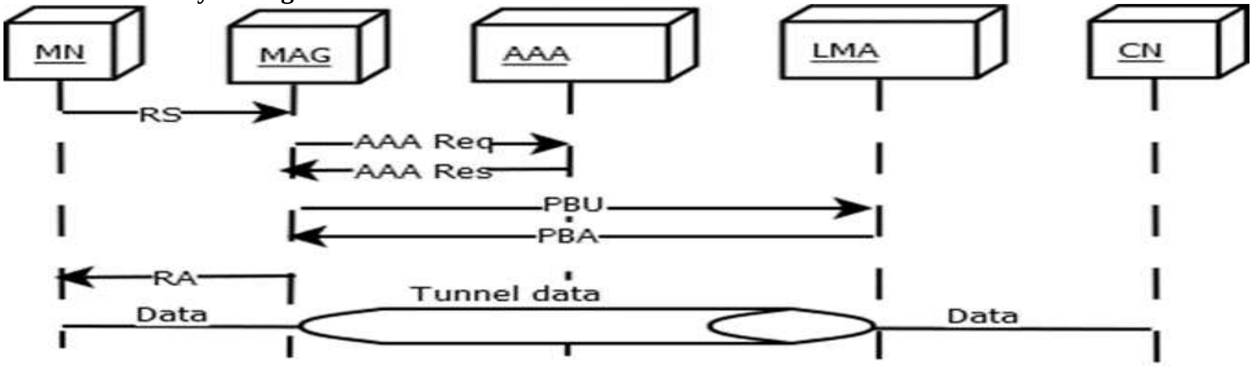

Figure 3:-Mobile node registration signaling call flow without controller.

According to the basic handover synchronisation scheme of the PMIPv6 protocol as shown in Figure 3, the handover delay corresponds to the connection time. Indeed, when the mobile disconnects to reconnect to a new attachment point, the registration process is triggered again as for a new connection, and can be expressed as follows [11]:

$$D = T_{Const} + T_A + T_{PU} \quad (1)$$

with: $T_{Const} = T_{WRS} + T_R$ (2)

T_{WRS}: is the delay between the establishment of the connection to the attachment point and the sending of the first packet.

$T_R = T_{RS} + T_{RA}$. T_{RS} and T_{RA} are made up of the propagation delay of the wireless channel and the service delay at the gateway.

$T_A$is the time taken to authenticate the mobile node to the AAA server and is defined as $T_A = T_{AAAres} + T_{AAAreq}$

T_{PU} is the time taken by the PBU and PBA messages, and can be defined as $T_{PU} = T_{PBU} + T_{PBA}$

Mobility management with SDN

case with a single controller for the domain.

Reactive mode

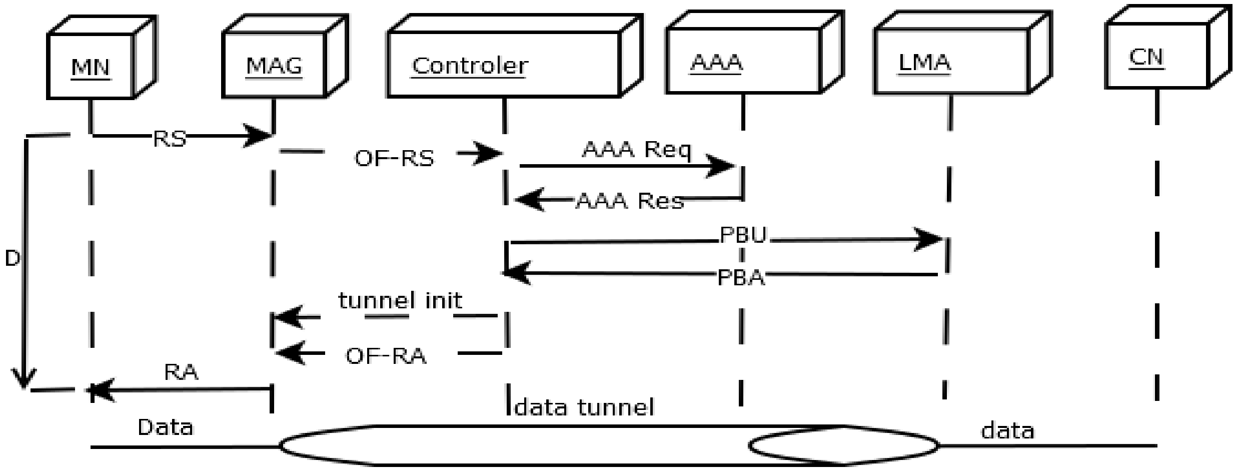

Figure 4:-Mobile node registration signaling call flow with a controller.

In SDN, the takeover delay is the reconnection time, and can be expressed as follows:

$$D = T_{Const} + T_{OF-R} + T_A + T_{OF-PU} \quad (3)$$

$T_{OF-R} = T_{OF-RS} + T_{OF-RA}$ where $T_{OF-RS} T_{OF-RA}$ and are the communication delays between the controller and the access point or MAG.

T_{OF-PU} is the time taken for the PBU and PBA messages to establish communication between the controller and the mobility anchor, and can be defined as $T_{OF-PU} = T_{PBU} + T_{PBA}$

In the configuration with the SDN paradigm we notice that an extra delay is added to equation 1 but this is only valid for the first connection, but once the mobile is on the move, the T_A delay becomes zero as the controller records and performs an automatic check at its level, so equation 2 becomes:

$$D = T_{Const} + T_{OF-R} + T_{OF-PU} \qquad (4)$$

Proposed Method:-

Our solution is based on an algorithm that is implemented on the controller of each domain; the algorithm of our approach is summarized in four steps:

- Step 1: initialization and detection of edge nodes (refer to Algorithm 1).
- Step 2: computation of distances between the mobile node and the edge nodes (refer to Algorithm 2).
- Step 3: selection of the visited domain (refer to Algorithm 3): If the distance between the mobile node and anedge node is equal to 1 then the attached domain is selected.Otherwise, go to step 2.
- Step 4: installation of the management rule onthe next destination node (refer to algorithm 3)

Algorithm 1:Detection of theedge nodes

```
Input: The network graph $G = (V, E), ou|V| = n$
Precondition: $a_{ij} = \begin{cases} 1 \text{ if} (v_i, v_j) \epsilon E \\ 0 \text{ otherwise} \end{cases}$ where $a_{ij}$ is the adjacency matrix of the graphG
$v_0$ is an SDN controller
Output: the set of edge nodes SEN
Begin
    For each node $v_i \in V$do
        For each node $v_j \in V$do
            if $a_{ij}$== $a_{i0}$ ==1 and $a_{0j}$ == 0 then
            $v_i$ is added to SEN
            End if
        End for
    End for
End
```

Algorithm 2: Computation of distances

```
Input: The network graph $G = (V, E), with|V| = n$
Precondition: $v_p$ is an access point and $succ[v_i]$ adjacency list of $v_i \in V$
$d_e$ is the distance between the access point and the edge node
Output: DIST= the distances between the access point and the edge nodes
    Begin
        $DIST = nil$
for each node $v_e \epsilon$ SEN do
        if $d_{p,e}$ = length of shortest path between $v_e$ and $v_p$
        $d_{p,e}$ is added to DIST
        End if
    end for
    end
```

Algorithm 3: Selection of the visited domain

```
    Input: The network graph $G = (V, E), ou|V| = n$ ;$D_i = \{ D_1, D_2, \dots, D_n\}$, $d_i = \{d_1, d_2, d_3, \dots, d_n\}$
    Precondition:m is a Boolean variable that indicates the change of MAG by the mobile node
    Output: next domain $D_\rho$
    Begin
    m=false
    Whilem == True
    //Compare ($d_i$)
    if $d_\rho == 1$ then
    return $D_\rho$ // the domain attached to edge node ρits chosen.
    if $d_\rho == 0$ then
      set up rules on next MAG
End
```

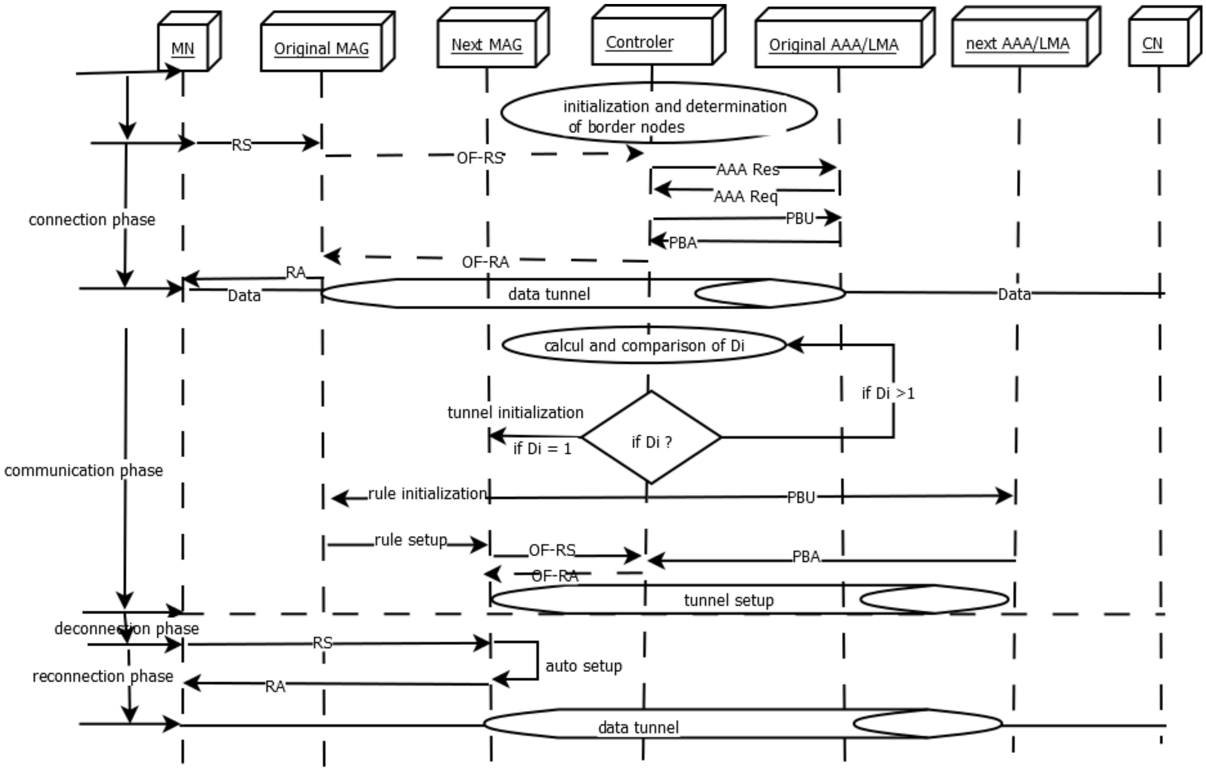

Figure 5:- Proactive OF-PMIPv6 handover signaling call flow.

Handover Latency

According to [15], equation (4) is used for a proactive solution:

$$D = T_{Const} + T_{OF-R} + T_{HO-wait} \quad (4)$$

With $T_{HO-wait}$ the additional communication delay between the controller and the visited domain anchor in the case of non-response from the latter to ensure that the mobile has arrived in the next domain.

In fact, the controller in the proactive mode communicates with the next MAG, anchor, and mobile node without waiting for a response from the first. The controller first sends the tunnel initialization message to the next MAG, then the PBU message to the anchor and, while waiting for the PBA message, it sends the forwarding request message to the mobile node via the Original MAG. This simultaneous communication allows us to reduce the handover delay, because when the controller receives the OF-RS message from the next MAG, it has already completed its communication with the anchor and immediately sends the OF-RA message. However, it may happen that the mobile node does not leave the domain and the installed rules expire after a certain time because the author has not considered the precision in the domain visited by the mobile and the time of arrival of the latter in the said domain. This generates a waste of resources that our method improves and reduces in other respects the delay of taking charge. This delay then strongly depends on the probability of exit of the domain of the node and can be expressed as follows:

$$Pt = \begin{cases} 0 & \text{if} v_d < T_{OF-R} \\ 1 & \text{otherwise.} \end{cases}$$

With v_d is the exit speed of the domain
L'équation (4) devient $D = T_{Const} + Pt(T_{OF-R} + T_{HO-wait})$ (5)

Packet loss
In order to evaluate packet loss, NO-PMIPv6 does not take into account packet buffering when the mobile disconnects from the OMAG.The value of packet loss during mobile movement between two domains is equal to the number of packets lost while the mobile is disconnected
$P_d = D * debit$ (6)

Simulations and results
Simulation setup
The proposed method was implemented usingMininet WIFI[20].The proposed method was integrated using some Mininet modules to create the topology, nodes, and controllers. The first part of the simulations aimed to study and reduce the handover delay when a node migrates from one domain to another. The second part aimed to study and reduce the packet loss rate during handover. The metrics used to evaluate the performance of the proposed method are defined as follows:

- Delay: Average end-to-end transmission delay during domain change (see Equation (5))
- Packet delivery rate: Ratio of the number of non-repeating packets delivered to the destination to the number of packets sent by the source (see Equation (6)).

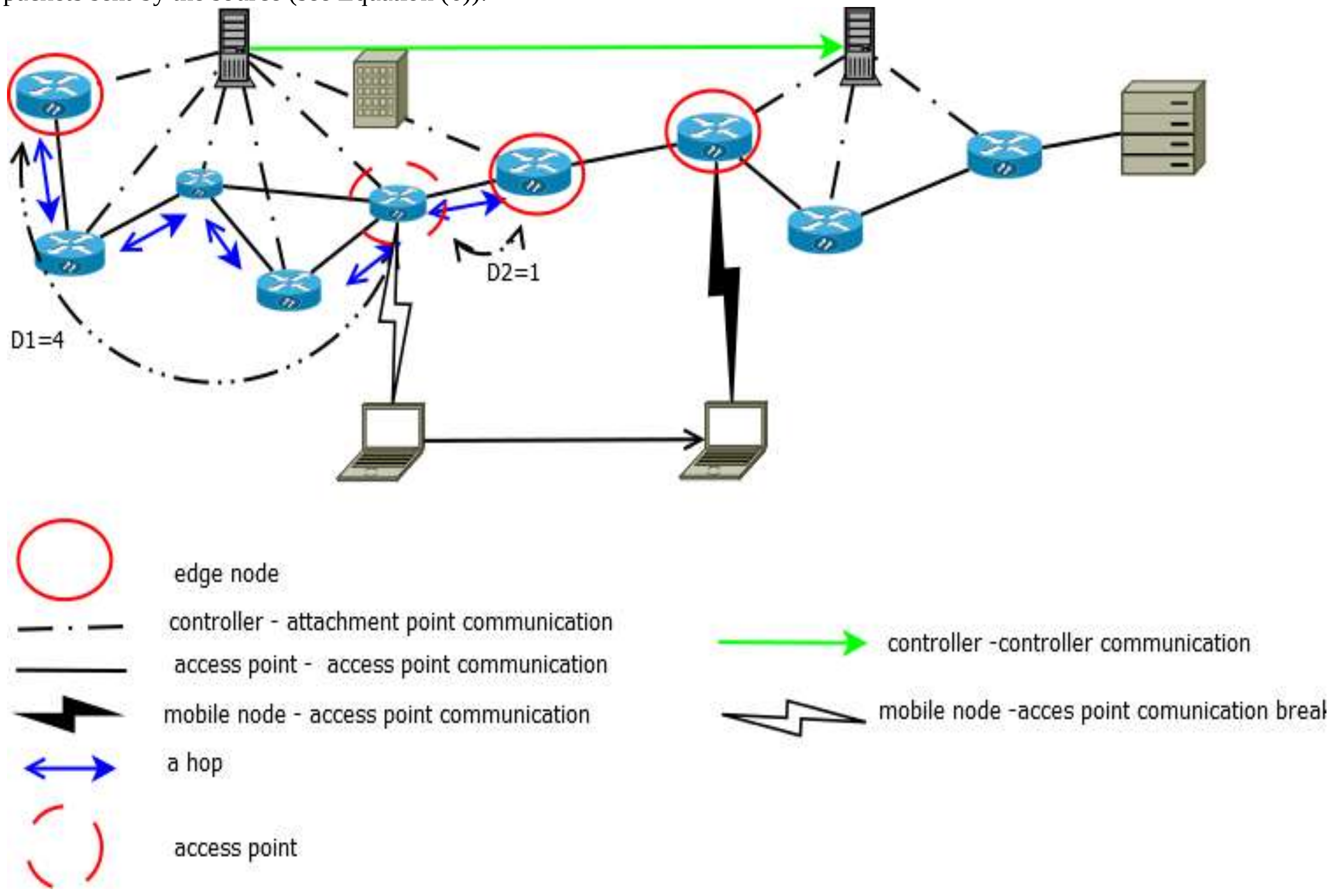
D2=1
D1=4
edge node
controller - attachment point communication
access point - access point communication
mobile node - access point communication
a hop
access point
controller -controller communication
mobile node -acces point comunication breal

Figure 6:-The simulated network topology.

The experimentation takes place in two steps.The first step is the implementation of algorithms 1 and 2. The commands used are "distance" and "ping" to obtain the position of the edge nodes and the mobile with respect to them.

In the second step, we record the results of the "ping" and "iperf" commands and evaluate the delays. The parametersof simulations are listed in the table and the results are shown in figure 7.

Table 2:- Parameters and descriptionof values simulation's.

Parameters	Description	Values
simulator	tools or software to virtualize an SDN network	Mininet-Wifi
Configuration	network parameters that respect the PMIPv6 protocol principle	PMIPv6
Architecture	design	SDN
mobility programming code	program source file	Mininet-wifi/mn_wifi/Mobility.py
SDN controller	C1=net.addcontroller('c1')	RYU
OpenFlow messages	communication protocol	V1.3
Traffic Generator	command to perform the tests	Ping ,iperf
Mobility model	Net.setpropagationModel(model="logdistance"...)	Straight line
Mobile speed	the ratio of the distance covered to the time	0,87m/s
Standard used	Wireless technology	802.11n, 100Mbits
jitter	time between packages	2,2ms
$D_{NO-PMIPv6}$	average support time for no-mipv6	0,5
$D_{OF-PMIPv6}$	average support time for of-mipv6	1,72

Our results were compared with those of [9].

Simulation results

Handover Latency Comparison

NO-PMIPv6 (i.e., our method) is a method that reduces the support time. Indeed, it implemented on the controller, is executed at the creation of the network to determine all the edge nodes (Algorithm 2).Then with the help of the strategic positions of the edge nodes, a computation is made with the access point which is used to register the mobile.Thispositionof mobile node is calculated at each displacement of the mobile to have permanently its position compared to the edge node. When the distance is equal to 1 then we deduce that the mobile is about to leave the domain for another. The second phase of our algorithm is triggered once the distance is equal to 1 by injecting management rules into the nodes that will be elected to take care of the mobile upon its arrival in the visited domain. Thus, when the mobile arrives in the visited domain, the pickup delay is reduced. as shown in Figure7 We determined this reduction by relating our results to those of [9], i.e.,$\frac{D_{NO-PMIPv\ 6}}{D_{OF-PMIPv\ 6}}$and the average of the results obtained gives us a reduction rate of 29.523%.$D_{NO-PMIPv\ 6}$ is the average obtained from the different delays of the solution times in the simulations $NO - PMIPv6$. $D_{OF-PMIP\ v6}$is the average obtained from the different delays of the solution times in the simulations $D_{OF-PMIPv\ 6}$.

Concerning the study with the loss of packets, we note that the results are proportional and depend on the delay of disconnection, the more the delay of disconnection is big more we have loss of packets. Indeed, we took the default jitter of the simulator which is 2.2ms between packets and the average obtained from the different delays of supported during the previous test are 0.5ms and 1.72ms respectively for the solutions of NO-PMIPv6 and OF-PMIPv6. Thus, when we extend the disconnection delay, our results remain better than those of [15] and the results are shown in Figure 8.

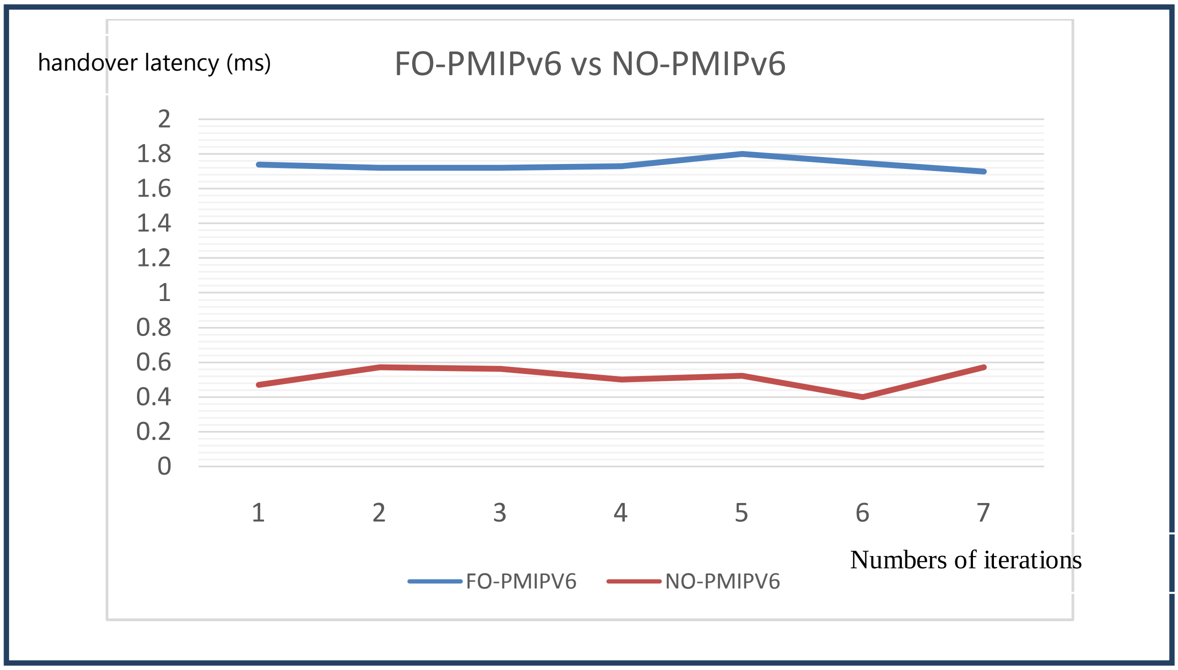

Figure 7:-Comparison of handover delays.

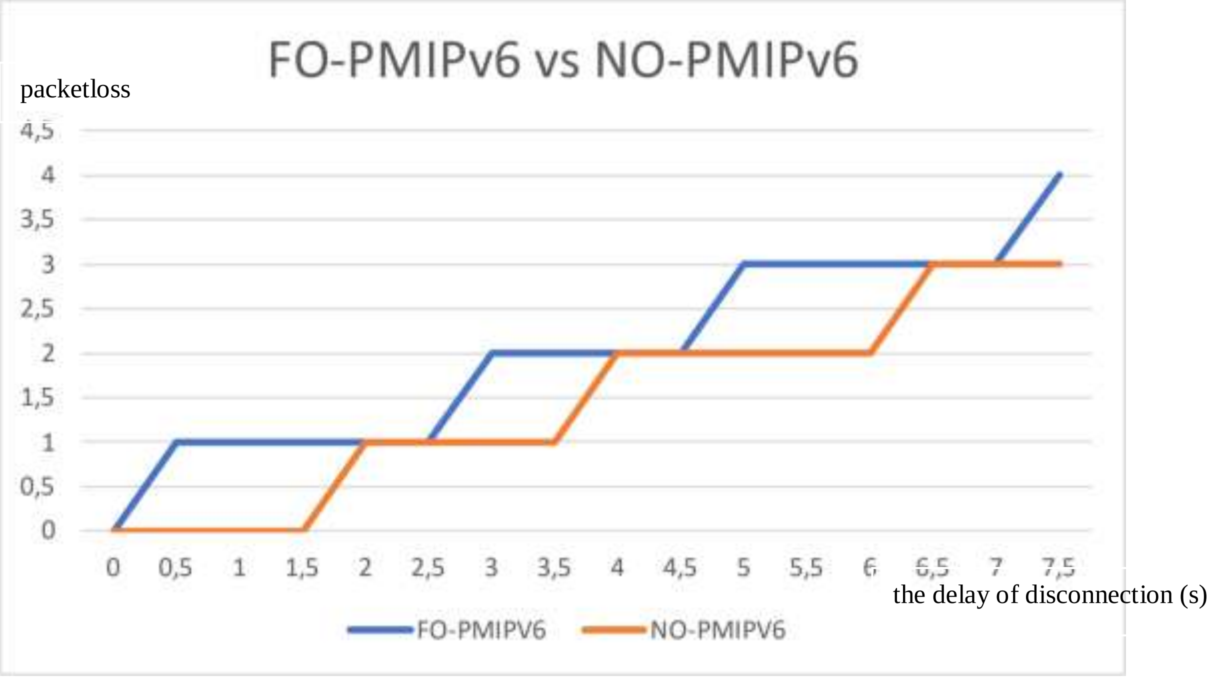

Figure 8:-Packet loss.

Conclusion Et Perspectives:-

In this paper, a mobility management method has been proposed for Wi-Fi networks based on SDN architecture.NO-PMIPv6 leverages edge nodes to anticipate the next destination of the mobile in a new domain and then chooses the most appropriate node in the next domain to host the mobile configuration before the mobile arrives.By using NO-PMIPv6, the handover delay of the mobile when it arrives in the visited domain is reduced compared to the OF-PMIPv6 method. The simulation results confirm that our method (i.e., NO-PMIPv6) is efficient in terms of handover latencyand at the same time reduces the packet losswith a rate between 0% and 50% as shown in Figure 8. This new method is suitable for different types of networks. Further work is needed to consider real-world conditions, i.e., deploying it on a campus or large areaWi-Fi network.

References:-

[1] A. Bradai, A. Benslimane, and K. D. Singh, “Dynamic anchor points selection for mobility management in Software Defined Networks,” Journal of Network and Computer Applications, vol. 57, pp. 1–11, Aug. 2015, doi: 10.1016/j.jnca.2015.06.018.

[2] N. Bouzakaria, M. Ghareeb, B. Parrein, and S. Rouibia, “Une architecture hybride Client/Serveur et Pair-à-Pair pour le streaming vidéo sur l’Internet.”

[3] C. E. Perkins, “MOBILE IP,” IEE Communication Magazine, vol. 35, no. 5, 1997.

[4] S. M. Ghaleb, S. Subramaniam, Z. A. Zukarnain, and A. Muhammed, “Mobility management for IoT: a survey,” Eurasip Journal on Wireless Communications and Networking, vol. 2016, no. 1. Springer International Publishing, Dec. 01, 2016. doi: 10.1186/s13638-016-0659-4.

[5] M. Siksik, H. Alnuweiri, and S. Zahir, “A DETAILED CHARACTERIZATION OF THE HANDOVER PROCESS USING MOBILE IPV6 IN 802.11 NETWORKS.”

[6] A. D. Johnson, C. Perkins, and J. Arkko, “Rfc 3775 Title Mobility Support in IPv6,” 2004. [Online]. Available: https://www.hjp.at/doc/rfc/rfc3775.html

[7] F. Belghoul, Y. Moret, and * -Christian Bonnet, “Mécanismes de handover pour les réseaux IP sans-fil.”

[8] D. Johnson, C. Perkins, and J. Arkko, “RFC 3775 - Mobility support in IPv6,” IETF, June, pp. 1–165, 2004, [Online]. Available: http://portal.acm.org/citation.cfm?id=236387.236400%5Cnhttp://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:RFC+3775#0

[9] S. Gundavelli Ed., K. Leung, v. Devarapalli, K. Chowdhury, and B. Patil, “Proxy Mobile IPv6,” 2008, Accessed: Oct. 10, 2021. [Online]. Available: https://www.hjp.at/doc/rfc/rfc5213.html

[10] K. H. Lee, H. W. Lee, W. Ryu, and Y. H. Han, “A scalable network-based mobility management framework in heterogeneous IP-based networks,” in Telecommunication Systems, Apr. 2013, vol. 52, no. 4, pp. 1989–2002. doi: 10.1007/s11235-011-9479-3.

[11] H. Yokota, K. Chowdhury, R. Koodli, and F. X. B. Patil, “Fast Handovers for Proxy Mobile IPv6,” 2010.

[12] Mun-Suk Kim a, SuKyoung Lee a, David Cypher b, and Nada Golmie b, “Performance analysis of fast handover for proxy Mobile IPv6,” 2012.

[13] Haneul Ko, Insun Jang, Jaewook Lee, Sangheon Pack, and Giwon Lee, 2017 IEEE International Conference on Consumer Electronics (ICCE)□ : date, 8-10 Jan. 2017., IEEE. 2017.

[14] D. Wu et al., “IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. XX, NO. XX, XX XXXX 1 Towards Distributed SDN: Mobility Management and Flow Scheduling in Software Defined Urban IoT.”

[15] S. M. Raza, D. S. Kim, D. Shin, and H. Choo, “Leveraging proxy mobile IPv6 with SDN,” Journal of Communications and Networks, vol. 18, no. 3, pp. 460–475, Jun. 2016, doi: 10.1109/JCN.2016.000061.

[16] M. Hata, S. Izumi, T. Abe, and T. Suganuma, “A proposal of SDN based mobility management in multiple domain networks,” 18th Asia-Pacific Network Operations and Management Symposium, APNOMS 2016: Management of Softwarized Infrastructure - Proceedings, 2016, doi: 10.1109/APNOMS.2016.7737263.

[17] Seong-Mun Kim, Hyon-Young Choi, Pill-Won Park, Sung-Gi Min, and Youn-HeeHan"OpenFlow-based Proxy Mobile IPv6over Software Defined Network (SDN)"Institute of Electrical and Electronics Engineers, 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC).doi: 10.1109/ccnc.2014.6866558

[18] Y. Li, H. Wang, M. Liu, B. Zhang, and H. Mao, “Software defined networking for distributed mobility management,” 2013 IEEE Globecom Workshops, GC Wkshps 2013, pp. 885–889, 2013, doi: 10.1109/GLOCOMW.2013.6825101.

[19] Y. Bi, G. Han, C. Lin, M. Guizani, and X. Wang, “Mobility Management for Intro/Inter Domain Handover in Software-Defined Networks,” IEEE Journal on Selected Areas in Communications, vol. 37, no. 8, pp. 1739–1754, Aug. 2019, doi: 10.1109/JSAC.2019.2927097.

[20] M. Tortonesiet al., Proceedings of the 11th International Conference on Network and Service Management (CNSM)□ : November 9-13, 2015, Barcelona, Spain.