Follow Me Cloud Concept Implementation Based on OpenFlow and PMIPv6 Mobility Management System

Abdelkader Aissioui
PRISM, University of Versailles
abdelkader.aissioui@ens.uvsq.fr

Mourad Guerroui
PRISM, University of Versailles
mourad.guerroui@prism.uvsq.fr

Adlen Ksentini
IRISA, University of Rennes1
adlen.ksentini@irisa.fr

ABSTRACT

The latest technological advances in mobile networks have achieved very high data rates. In parallel, services are increasingly provided and hosted on cloud computing systems. These services are often hosted in geographically distributed data-centers, or federated clouds. Within a 3GPP mobile network, the more the distance between the client and the service increases, the more the QoE decreases. In this paper, we present Follow Me Cloud (FMC) concept, in which services are migrating according to the user’s movements to ensure the best QoE. We propose an implementation of this technology in IPv6 mobile networks. Particularly, the solution is based on SDN paradigm and PMIPv6 mobility management system.

Categories and Subject Descriptors

Keywords

1. INTRODUCTION

Mobile data traffic has surged over the last years, increasing pressure on the operators’ core networks. As a result, mobile operators are facing a tremendous challenge to accommodate these huge mobile traffic volumes, stressing more and more the mobile networks already in capacity crisis. To cope with this ever-growing mobile traffic, mobile operators are looking into cost-effective solutions that require minimal investment in their infrastructure and can accommodate such a large amount of mobile network traffic. The first phase of overcoming this data challenge is to move Internet traffic off the mobile core network. Data offload is a critical issue for both 3G and LTE mobile broadband networks. Traffic can either be offloaded from the Radio Access Network (RAN) or from the core network. Selective IP Traffic Offload (SIPTO) is a prominent solution that addresses the need to break out traffic closer to RAN including Femtocells and WiFi, but the biggest benefits come in the form of offloading traffic from the core. The Long Term Evolution-Evolved Packet Core (LTE-EPC) network has the ideal architecture to realize these benefits.

As regards mobility, Proxy Mobile IPv6 (PMIPv6) [1] has been standardized by IETF, and widely adopted in 3GPP architecture. Taking advantage of the network-based mobility management, PMIPv6 enables IP mobility for moving hosts without their involvement. Compared to the host-based mobility management (e.g. Mobile IPv6 or MIPv6 [2]) PMIPv6 brings some benefits such as: (i) avoiding the complexity of protocol stack in the MN; (ii) supporting mobility without the involvement of the MN; and (iii) reducing tunneling overhead and decreasing handover latency. On the other hand, service provisioning, today, finds in the emerging Cloud Computing paradigm a flexible and economically efficient solution, in particular for small and medium enterprises that do not want to invest huge capitals for creating and managing their own IT infrastructures. The basic tenet of cloud computing is that end users do not need to care about where a service is actually hosted, while service providers may dynamically acquire the resources they need for service provisioning in a pay-per-use model. While for most of elastic web applications the relative position of client and server end systems does not affect the perceived Quality of Experience, provided enough bandwidth is available in the end-to-end path connecting clients with servers, rich interactive applications are sensible to other communication metrics, such as delay and jitter. In the absence of explicit QoS control mechanisms in the network, the only way to improve Quality of Experience is to locate servers as close as possible to user terminals. Such an approach, largely exploited by Content Delivery Networks, can be further advanced in the era of Cloud Computing. Assuming that several cloud-enabled datacenters are made available at the edges of the Internet, service providers may take advantage of them for optimally locating service instances as close as possible to their users. In such a context, mobility of user terminals makes such location decisions even more difficult.

In this paper, we present Follow Me Cloud (FMC) concept a technology that allows the relocation of services provided to users depending on their movements. Services are therefore always provided from data center locations that are optimal for the current locations of the users. This provides users with improved Quality of Service/Quality of Experience, at the same time, it allows preserving operators’ network resources by escaping network traffic to data centers through the nearest points compared with users’ locations.

Another advantage of the follow-me cloud technology is that migration of services is seamless and transparent to users. On-going sessions between users and services are not interrupted and connections do not need to be reestablished, even if users and/or servers (i.e., hosting services) change location.

In the present paper we propose a solution to implement the concept of Follow Me Cloud in a mobile IP context, and more specifically, in IP mobility domains supporting Proxy Mobility IPv6 (PMIPv6) as mobility management protocol. These PMIPv6 domains are interconnected through the mobile operator core networks to service provider networks provisioned in data-centers or Clouds.

The approach we propose is composed of two parts (1) The first is to implement a PMIPv6 inter-domain mobility support that interacts with a system based on SDN/OpenFlow, in which customers mobility information are pushed (2) The second part is an architecture based on SDN/OpenFlow, it exploits the mobility information delivered by the PMIPv6 inter-domain mobility support and can trigger
services/sessions migration in the data-center/cloud side in order to ensure an improved QoS/QoE to users.

Given the fact that current PMIPv6 protocol fails to support inter-domain mobility management, we are going to rely on the concept of DMM (Distributed Mobility Management) to introduce an inter-domain PMIPv6 mobility support [4]. This PMIPv6 inter-domain mobility support interfaces with a system of controllers and routers (Data Center Gateway) based on SDN/OpenFlow to achieve the concept of Follow Me Cloud. The solution permits removing the complexity and workload associated with the use of tunnels in the management of mobility through the update of routers’ routing table using OpenFlow.

The rest of this paper is organized as follows. We discuss related work in section 2. In section 3 we present our improvement to support FMC-PMIPv6 inter-domain mobility management, next we introduce our FMC based OpenFlow solution in section 4. Section 5 provides performance analysis of signaling cost, handover latency and tunnel usage. Finally, in section 6 we conclude and present future work.

2. RELATED WORK

Live migration of services is a hot topic in modern virtualization technologies, the use of this feature was introduced in recent hypervisors, and it allows the move of an entire running Virtual Machine from one physical host to another without downtime, the VM then retains all these network established sessions ensuring thereby a seamless migration process. Within 3GPP mobile networks the need of service migration is often triggered by users’ movements. There is therefore a strong correlation between the Mobility Management Protocol of the mobile network (the mobile network operator side) and the cloud management framework (the cloud or service provider side) to realize service migration. As part of this work, we exploit this correlation by the combination of the two parties to implement the Concept of FMC.

In the literature several works have been proposed. In [1] "Interactions between PMIPv6 and MIPv6: Scenarios and Related Issues" the authors present a scenario in which PMIPv6 is used for the management of intra-domain mobility while MIPv6 is used as manager inter-domain mobility. This method provides additional complexity to mobile clients because they must support two protocol stacks network-based and host-based.

In [2] "I-PMIP: An Inter-Domain Mobility Extension for Proxy Mobile IPv6" extension for PMIPv6 is proposed to support inter-domain mobility reusing the LMA (Local Mobility Anchor) as a global mobility manager (global anchor points) when the mobile is outside its home network. Traffic is being forwarded to / from the session mobility anchor (SMA) to/from the current serving mobility anchor (LMA-S) at which the mobile is currently attached. The disadvantage of this method is that the proposed mobility service is based on the user (user-based), so that the mobility service is always applied, even for services that do not require (sub-optimal routing, load problems related to tunneling).

The [3] "Network -based Inter -domain handover Support for PMIPv6" approach is based on the idea that home-address (HoA) and Care-of-Address (CoA) are not only used for MN (mobile node) but also for the CN (corresponding node). Two ECB (Binding Cache Entry) by MN are reported on PMIPv6 domain elements, one for intra-domain mobility (equivalent to PMIPv6 BCE), and the other for inter-domain mobility latter maintains the binding HoA-CoA from correspondent node (CN). When migrating to another PMIPv6 domain, the S-LMA (serving LMA) should contact the former LMA for the HoA of CN. It also comes in contact with the LMA home CN to update the location of the MN. This method has the advantage of the quasi-optimal routing traffic (CN directly to the MN’s current position), however, it becomes too complicated when the MN communicates with multiple CN simultaneously. In addition, it can only be applied to mobile attached to PMIPv6 domains.

Authors of [4] "DMM-based Inter-domain Mobility Support for Proxy Mobile IPv6" presented an inter-domain mobility solution based on the concept of distributed management of mobility (DMM: Distributed Mobility Management). The basic idea of the DMM is to bring the LMA nodes (Local Mobility Anchors) closest to the mobile clients. Thus avoiding sub-optimal routing, load related to signaling traffic (Control Plan), and while providing a dynamic service mobility. Two approaches have been proposed, partially distributed or totally distributed. In the first approach the ICMD (Inter-domain Central Mobility Database) is used to record the mobility information sessions all PMIPv6 domains. When a MN migrates to a new domain PMIPv6, the current LMA (LMA-S) allocates a new prefix (Pref2) and sends a PBU (proxy binding update) to ICMD for the registration of the new prefix. Upon receipt of the PBU, the ICMD updates the position of MN in the BCE table. And in turn, it sends a PBU to the former A-LMA LMA by inserting the address of S-LMA to update the position of MN. A bi-directional tunnel is then created to forwarder traffic from/to the MN using the address Pref1.

3. PROPOSED ARCHITECTURE

The solution we propose in this paper is to implement the concept of Follow Me Cloud in a mobile context, more specifically in mobility domains managed by the PMIPv6 protocol. These PMIPv6 mobile network domains are interconnected through operator core networks to service provider networks in Data-Center or Clouds. Thus, our solution OF-FMC-PMIP is a framework that combines mobile operator core network and services provider network in the goal to enables mobile cloud services to follow their respective mobile users during their motilities by migrating all or portions of services to the optimal DC to ensure them the best QoE/QoS.

The proposed approach OF-FMC-PMIP is composed of two parts: (I) The first is to implement a PMIPv6 inter-domain mobility support that interacts with a system based on SDN/OpenFlow, to which users mobility information are pushed (II) The second part is an architecture based on SDN/OpenFlow, it exploits the mobility information delivered by the PMIPv6 inter-domain mobility support and can trigger services/sessions migration in data-center/cloud level in the goal of improving QoE/QoS of end-users.

Given the fact that current PMIPv6 protocol fails to support inter-domain mobility management, we are going to rely in our approach on the work of [4] in which a DMM (Distributed Mobility Management) inter-domain PMIPv6 mobility support was introduced. This PMIPv6 inter-domain mobility support will be extended to interface with a system of controllers and
routers (Data Center Gateway) based on SDN/OpenFlow to achieve the concept of Follow Me Cloud. The solution permits removing the complexity and workload associated with the use of tunnels in the management of mobility through direct routing using OpenFlow protocol to push new routes on the OpenFlow-enabled elements of the SDN/OpenFlow architecture.

4. OF-FMC-PMIPv6 FUNCTIONING

In this section we define the elements of our solution OF-FMC-PMIPv6 and describe the operations performed by the two parts of the architecture and their elements.

4.1 OF-FMC-PMIPv6 ELEMENTS

- **MN** (Mobile Node): a moving node.
- **CN** (Correspondent Node): a node in communication with the MN.
- **pLMA** (previous Local Mobility Anchor): the former mobility anchor for MN.
- **nLMA** (new Local Mobility Anchor): the new mobility anchor for MN.
- **IDMD** (Inter Domain Mobility Database): the mobility information database, it has a Binding Cache Entry.
- **BCE** (Binding Cache Entry): a table containing information about the mobility of MN.
- **FMCC** (Follow Me Cloud Controller): FMC controller based on SDN/OpenFlow.
- **DCG** (Data Center Gateway): the gateway of the Data-center or Cloud.
- **DMAM** (Decision Making Application Module): the module responsible to take decision about the relevance of service migration.
- **MIGW** (Mapping Information Gateway): the node possessing mapping information between the Local Mobility Anchor Gateway LMA (PGW for EPS system) and the Data Center Gateway DCG

4.2 INTER-DOMAIN MOBILITY SUPPORT

The PMIPv6 inter-domain mobility support we propose builds on the work done in [4], we extend this one by a new module that interacts with the FMCC OpenFlow controller to which mobility information are pushed, and then used to trigger migration service on the cloud according to user mobility.

We define two global entities, one for the mobile network side called IDMD and the other for cloud provider network side called FMCC. a) Inter-Domain Mobility Database IDMD ensures the registration of mobility information of all PMIPv6 domains, and informs the FMCC about MN inter-domains movements (b) Follow Me Cloud Controller FMCC utilizes the mobility information delivered by the IDMD. It collaborates with the DMAM module in order to choose the most appropriate datacenter which offers the best QoS/QoE for users according to their movements and locations. It is noted that DMAM interact with MIGW holding mapping information between the mobile core network and the service provider network (LMAs or PGWs DCG mapping).

4.2.1 INITIAL REGISTRATION OF A MN

Upon the first attachment of a MN to a PMIPv6 domain, the PMIPv6 standard operations are executed. Then, the domain’s LMA sends a PBU (Proxy Binding Update) to the IDMD containing (MN-id, pref1), it creates an entry in its BCE table as (MN-id, pref1, LMA) and returns an PBA (Proxy Binding Acknowledgement) to the domain’s LMA.

- **The state of the IDMD Binding Cache Entry**

<table>
<thead>
<tr>
<th>ID</th>
<th>Prefix</th>
<th>A-LMA</th>
<th>S-LMA</th>
</tr>
</thead>
<tbody>
<tr>
<td>MN</td>
<td>prefix1</td>
<td>pLMA</td>
<td>nLMA</td>
</tr>
</tbody>
</table>

4.2.2 INTER-DOMAIN OPERATIONS

When a MN moves to another PMIPv6 domain, the new LMA (nLMA) allocates it a second prefix (pref2) and sends a PBU to IDMD to register the new prefix2. Upon receiving the PBU, IDMD updates its BCE table with the new location of the MN, and adds a new entry for the new prefix2. Then, the IDMD sends a PBU to pLMA with (MN-id, nLMA), once received, the plMA creates the endpoint for bi-directional tunnel with nLMA, updates its BCE table, its routing table for prefix1 and it responds with a PBA. The IDMD used as proxy returns a PBA with the address of the plMA to nLMA that performs in its turn the same operations as the plMA, and then a bi-directional tunnel is established between plMA and nLMA to carry the traffic from/to prefix1 MN address.

At the same time, when the IDMD receives PBU for an MN inter-domain mobility registration, and upon the allocation of its prefix2 in the new domain, the IDMD sends a SESSION-MIGRATION-REQUEST message to the FMCC. This message contains information about MN-ID, its allocated prefixes and on which LMAs are allocated. This message is used to alert FMCC and IDMD about the MN inter-domain movement and the eventualty of triggering a service migration on the cloud side.

- **The state of the Binding Cache Entry IDMD**

<table>
<thead>
<tr>
<th>ID</th>
<th>Prefix</th>
<th>A-LMA</th>
<th>S-LMA</th>
</tr>
</thead>
<tbody>
<tr>
<td>MN</td>
<td>prefix1</td>
<td>pLMA</td>
<td>nLMA</td>
</tr>
<tr>
<td>MN</td>
<td>prefix2</td>
<td>nLMA</td>
<td>-</td>
</tr>
</tbody>
</table>

Global mobility information are maintained by the IDMD, when the pLMA receives a packet destined to the prefix1 address, it forwards it through the tunnel to the nLMA in the new PMIPv6 domain.

4.3 ARCHITECTURE BASED ON SDN/OPENFLOW FOR FOLLOW ME CLOUD

This section presents the SDN/OpenFlow architecture we propose, that permits to generate/handle the control traffic (control plane) to provide seamless migration of services in the cloud side to mobile nodes. This means that the MN will be totally unaware of this migration, therefore all its ongoing sessions/services (data plane) will be kept active and will not be lost.

4.3.1 THE ELEMENTS OF SDN/OPENFLOW ARCHITECTURE

FMCC: FMC Controller is the brain of the architecture, in our solution it is in the premises of service provider FMC. It can be owned and operated by the mobile network operator MNC or a third party. FMCC operates the information of users mobility provided by the IDMD database following the inter-domain mobility of MNs. The FMCC supports the OpenFlow protocol to modify the behavior of SDN network devices by generating the necessary control traffic (control-plane) to
ensure a transparent service migration on the cloud side. It is based on the analysis realized by Decision Making Application Module DMAM and on the Mapping Information Gateway MIGW between the Local Mobility Anchor LMA (PGW for EPS system) and the Data Center Gateway DCG (LMAs or PGWs ↔ DCG) in order to estimate the relevance of service migration, and consequently, select the optimal target datacenter if the migration is deemed appropriate.

- **DCG**: Data Center Gateway represents the network gateway on the Data Center or cloud provider side. DCG is OpenFlow-enabled device supporting OpenFlow protocol. As the model of cloud service proposed in this paper is delivered by geographically distributed federated DCs, we will consider having one DCG by datacenter site.

- **pLMA/nLMA**: previous Local Mobility Anchor/new Local Mobility Anchor, are the anchors points of mobile network, in the context of the Evolved Packet System (EPS) these anchors points are represented by the Packed Data Network Gateways (PDN-GWs) elements of mobile core network. In this work these elements are supposed OpenFlow-enabled therefore supporting OpenFlow protocol.

### 4.3.2 CONTROL OPERATIONS FOREGOING THE SERVICE MIGRATION

As we have seen above, IDMD is the overall entity maintaining the information of users’ mobility, when a MN moves to a new PMIPv6 domain, the IDMD acts as a trigger for possible migration of service in the cloud side. Indeed, the change of PMIPv6 mobility domain is often associated with a change of anchor point (PGW for EPS or LMA for PMIPv6) and therefore the associated datacenter or cloud service.

This trigger plays a notifier role that signals a possible presence of a datacenter, which can provide improved QoS/QoE to MN in its new domain. Upon reception of PBU for an MN inter-domain mobility registration, the IDMD sends a SESSION-MIGRATION-REQUEST (Session Migration Request) message to the FMCC. This message contains information about MN-ID, its allocated prefixes (prefix1, prefix2, …) and on which LMAs are allocated. This message is used to alert FMCC about the MN inter-domain movement. When received by FMCC this one recognizes that there has been a MN inter-domain movement and that a decision about service migration must be taken.

In turn, the FMCC by relaying the SESSION-MIGRATION-REQUEST message activates the Decision Making Application Module DMAM which is responsible of decision making on whether a service migration is worthwhile or not, and consequently to select the new optimal target datacenter (DCG). The DMAM performs a series of analysis based on MN’s prefixes (pref1, pref2, …) and mapping information (between LMAs or PGWs ↔ DCG) by sending a GET-MAPPING-INFORMATION message to MIGW entity in order to get the last mapping information update (if it is not done yet) to which it responds with a POST-MAPPING-INFORMATION message.

The DMAM making decision process may be based on the service type (e.g., an ongoing video service with strict QoS requirements may be migrated) [12], content size (e.g., when a user has been watching a movie and the movie is about to finish at the time of LMA/PGW relocation, the DMAM may decide, to not initiate the service migration), task type of the
service (e.g., in case of MTC, in a session of emergency warning services, delay-sensitive measurement reporting services always have to be migrated to the nearest DC), and/or user class. It is worth noting that DMAM, the module in charge of the service migration decision relies on several attributes/criteria (could be conflicting) that depend on the user’s expectation on the service, QoS/QoE, cost, and network/cloud provider policies (at each LMA/PGW relocation, load balancing, maximize use of DC resources). Accordingly, to migrate a service or not can be defined as a multi-attribute decision making (MADM) issue, and solved by any relevant algorithm in this area which is out of scope of the present paper.

Once the service migration is deemed appropriate, the DMAM responds by a SESSION-MIGRATION-APPROVED message to the FMCC approving thus the service migration and instructing the FMCC to generate the essential control-plane traffic to ensure a seamless service migration. This is achieved by creating, pushing and installing OpenFlow rules on all components of the SDN architecture.

In the same time, the DMAM issues a SESSION-MIGRATION-REQUEST message to the source DC (DC1) and to the newly selected DC (DC2) requesting them to perform the migration of services related to (MN-ID, prefix1) from DC1 to DC2. Following this, the source datacenter DC1 forwards required content and/or exchanges adequate state information with the newly selected datacenter DC2. It should be noted that depending on the data size, data migration can be performed using one or more suitable robust and fast data delivery technologies. Finally, the session/service migration takes place on the new optimal target datacenter DC2. For its part, the FMCC continues by relaying the SESSION-MIGRATION-APPROVED message to the IDMD which uses it to update the location of the MN’s prefix1 address on its local BCE. In parallel, it generates and pushes the OpenFlow rules on the elements of the OpenFlow/SDN architecture.

4.2.3 OPENFLOW RULES OF CONTROL-PLANE TRAFFIC

We begin by defining the parameters used to create the necessary OpenFlow rules.

Prefix1: represents the IP1 of MN allocated by LMA1 in the PMIPv6 domain1.
Prefix2: represents the IP2 of MN allocated by LMA2 in the PMIPv6 domain2.
Prefix3: represents the IP of the CN in the cloud service provider domain.
DCG-src, DCG-dst: represents the source and destination datacenter of the service migration.

The idea behind the application of these OpenFlow rules is to ensure traffic redirection without packets loss according to the following criteria:

- (1) Outgoing Traffic: from Prefix1 (MN) \(\rightarrow\) to Prefix3 (CN); the traffic is routed to the new DC, therefore the DCG-dst.
- (2) Incoming Traffic: from Prefix3 (CN) \(\rightarrow\) to Prefix1 (MN); the traffic is routed to the new LMA, therefore the nLMA.
The following table defines the OpenFlow rules to push through the FMCC on each of the SDN architecture components.

Table 1: The applied OpenFlow rules by equipment

<table>
<thead>
<tr>
<th>Outgoing Traffic</th>
<th>Incoming Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic is routed to DCG-dst, instead of being forwarded via the tunnel!</td>
<td>Traffic is routed to the MN via the nMAG (traffic routing unchanged)</td>
</tr>
<tr>
<td>Traffic is routed to DCG-dst, instead of DCG-src.</td>
<td>Traffic is forwarded through the tunnel to nLMA and then is sent to the MN (traffic routing unchanged)</td>
</tr>
<tr>
<td>Traffic is routed to the CN after migration (traffic routing unchanged)</td>
<td>Traffic is routed to the nLMA then is sent to the MN</td>
</tr>
</tbody>
</table>

We identify four rules to be applied to the four entities of the SDN/OpenFlow architecture, R1, R2, R3 and R4.

- The application of rules R1 and R4 must be permanent, to route traffic of the nLMA to DCG-dst (R1) and conversely DCG-dst to nLMA (R4).
- The rules R2 and R3 are used to route traffic in transition during the service migration from DC1 to DC2. In order to not lose that traffic, these routing rules allow traffic to redirect to the new destination (DCG-dst) seamlessly and without packet loss. Hence the application of these rules is temporary, thus, they can be removed under request of the FMCC once the migration is successful and redirected traffic has stabilized.

5. EVALUATION AND PERFORMANCE ANALYSIS

In this section, we present the evaluation of OF-FMC-PMIP our approach for FMC concept implementation through a theoretical analysis. We select I-PMIP and DP-PMIP (only in its DP-PMIP-P variant) as benchmarks to be compared with our solution for its inter-domain management support part. This choice is motivated by the fact that the two solutions can provide inter-domain mobility support, and that our approach relies on a central database for inter-domain handover (ICMD in DP-PMIP and VMA in I-PMIP). The factors considered for this analysis are signaling cost, data exchange latency and tunnel usage.

5.1 NETWORK MODEL

In order to analyze the performance of our proposed solution we assume a network topology model as in Figure 4. We assume for simplifying, that the average distance in number of hops between entities is defined as follows:

- The distance between the PMIPv6 elements in the same domain is $d_i$ (e.g. between MAG and LMA).
- The distance between two domains is $d_i$ (e.g. between two LMAs).
- The distance between the MN and its MAG is $d_{iM}$.

5.2 DATA EXCHANGE LATENCY

The Data Exchange Latency (DL) depends on the route path the data takes between a MN and its CN. This evaluation is conducted through the comparison of the data path cost of the different approaches.

5.2.1 DATA DELIVERY PATH FOR INTRA-DOMAIN HANDOVER

In this case, the data path is the same as PMIP and data is exchanged via the LMA for all approaches.

$$DL_{OF-PMIP} = d(MN,MAG1)+d(MAG1,LMA1) + d(LMA1,DCG1)+d(DCG1,CN)$$ (1)

$$DL_{OF-PMIP} = d(MN,MAG1)+d(MAG1,LMA1) + d(LMA1,DCG1)+d(DCG1,CN)$$ (2)

$$DL_{OF-PMIP} = d(MN,MAG1)+d(MAG1,LMA1) + d(LMA1,DCG1)+d(DCG1,CN)$$ (3)

$$DL_{OF-PMIP} = DL_{OF-PMIP} = DL_{OF-PMIP} = d_{iM} + d_i + d_i$$

5.2.2 DATA DELIVERY PATH FOR INTER-DOMAIN HANDOVER

The data path is the same for I-PMIP and DP-PMIP and the inter-domain traffic is forwarded through the tunnel between LAM1 and LMA2 before joining the MN.

$$DL_{OF-PMIP} = d(MN,MAG2)+d(MAG2,LMA2) + d(LMA2,LMA1)+d(LMA1,DCG1)+d(DCG1,CN)$$ (4)

$$DL_{OF-PMIP} = d(MN,MAG2)+d(MAG2,LMA2) + d(LMA2,LMA1)+d(LMA1,DCG1)+d(DCG1,CN)$$ (5)

$$DL_{OF-PMIP} = DL_{OF-PMIP} = DL_{OF-PMIP} = d_{iM} + d_i + d_i$$
For OF-FMC-PMIP we distinguish two situations.

a) Before the $T_{\text{FMC}}$ delay ($t \leq T_{\text{FMC}}$)
\[
DL_{\text{inter-cust}} = d(MN,MAG2)+d(MAG2,LMA2) +d(LMA2,LMA1)+d(LMA1,DCG1) +d(DCG1, CN)
\]
\[
DL_{\text{intra}} = d_d + 2d_l + 2d_i
\]
\[
DL_{\text{PMIP}} = d_d + d_l + 2d_i, \quad \text{if } t \leq T_{\text{FMC}}
\]
\[
DL_{\text{OF-MC-PMIP}} = d_d + 2d_l + 2d_i, \quad \text{if } t \leq T_{\text{FMC}}
\]

5.3 SIGNALING COST

Signaling cost of a mobility management protocol is defined as the cost of signaling transmission associated to location update when an MN performs handovers. We use session-to-mobility (SMR) ratio the well-known factor which represents the relative ratio of session arrival rate to the user mobility rate. It is assumed that the subnet residence time (MAG subnet) and the session duration follow an exponential distribution with parameter $\eta$ and $\mu$ respectively. Therefore the SMR factor is calculated as $\rho_s = \frac{\eta}{\mu}$ [12]. Each LMA coverage area is supposed to be circular with $N$ subnets. According to [13], the intra-domain and inter-domain handoff probability are defined as $\rho_s = \frac{\eta}{\mu}$, $\rho_{\text{inter}} = \frac{1}{\rho \sqrt{N}}$. And the expected numbers of intra-handoff and inter-handoff are:
\[
E_{\text{intra}} = \frac{1}{\rho \sqrt{N}} \cdot E_{\text{inter}} = \frac{1}{\rho}
\]
thus, the average location signaling update is given by
\[
C = (E_{\text{intra}} - E_{\text{inter}})C_{\text{intra}} + E_{\text{inter}}C_{\text{inter}}
\]
where $C_{\text{intra}}$ and $C_{\text{inter}}$ are signaling update cost for intra-domain and inter-domain handover. Although different signaling messages have different size, we assume that they have the same size for simplicity. Also, the cost for transmitting a signaling message is supposed to be proportional to the distance between source and destination. The proportion is $a$ for wired and $a * \beta$ for wireless link.

It is easy to conclude the following equations for the three compared approaches for intra-domain and inter-domain handover.
\[
C_{\text{intra}} = 2a(\delta_d + 2\delta_l)
\]
\[
C_{\text{intra}}^{\text{OF-FMC-PMIP}} = 2a(\delta_d + 2\delta_l + 4\delta_i)
\]
\[
C_{\text{intra}}^{\text{OF-FMC-PMIP}} = 2a(\delta_d + 2\delta_l + 5\delta_i)
\]

5.4 HANDOVER LATENCY

The Inter-domain handover latency $D_{\text{inter}}$ is defined as the total time taken to complete all the operations before the traffic can be forwarded to the current location of the MN. Let $D_{\text{intra}}$

denote intra-domain handover delay. Then, the average value of handover latency is
\[
D = (\rho_{\text{intra}} - \rho_{\text{inter}})D_{\text{intra}} + \rho_{\text{inter}}D_{\text{inter}}
\]

Since the delay between two nodes depends on the bandwidth, the propagation delay and the distance between them, for simplicity, we suppose that the delay is proportional to the distance. The proportion is $\tau$ for wired link and $\tau \cdot \delta$ for wireless link. Let $t_2$ denote the delay caused by Layer 2 handover. Thus, the intra-domain handover delay of 1-PMIP, DP-PMIP, and OF-FMC-PMIP is the same (PMIP handover delay) and is calculated as follows:
\[
D_{\text{intra}}^{\text{1-PMIP}} = D_{\text{intra}}^{\text{DP-PMIP}} = D_{\text{intra}}^{\text{OF-FMC-PMIP}} = t_2 + 2\tau r \delta_d + 2\delta_l
\]
\[
D_{\text{inter}}^{\text{1-PMIP}} = t_2 + 2\tau r \delta_d + 2\delta_l + 4\delta_i
\]
\[
D_{\text{inter}}^{\text{DP-PMIP}} = D_{\text{inter}}^{\text{OF-FMC-PMIP}} = t_2 + 2\tau r \delta_d + 2\delta_l + 2\delta_i
\]

5.4 TUNNEL USAGE

In this subsection, we will measure the tunnel usage ratio, called $\theta$ which is defined as the ratio between the number of sessions using the tunnel (between the anchored and the current domain) and the total number of sessions. Therefore, it can be used to compare the overhead associated to tunnel use and showing the advantage of using OF-FMC-PMIP approach.

In 1-PMIP the inter-domain traffic always passes through the tunnel between the anchor point and the current one, therefore $\theta$ is equal to 1.
\[
\theta_{1-PMIP} = 1
\]

To measure $\theta$ in case of DP-PMIP, and OF-FMC-PMIP the sessions are separated into the new sessions and the handoff sessions. Let $N_s(t)$ and $N_h(t)$ respectively denote the numbers of the new sessions and handoff sessions up to time $t$. We suppose that $N_s(t)$ and $N_h(t)$ are a Poisson process with parameter $\lambda_s$ and $\lambda_h$, respectively. Then, we have
\[
\theta = \frac{N_s(t)}{N_s(t) + N_h(t)}
\]
According to [12] $\lambda_s = E[H] \lambda_s$, where $E[H]$ is the expected handoff number (in our case $E[H] = \frac{1}{\rho \sqrt{N}}$)

For the D-PMIP solution we obtain:
\[
\theta_{DP-PMIP} = \frac{1}{1 + \rho \sqrt{N}}
\]
And for OF-FMC-PMIP approach we obtain:
\[
\theta_{OF-FMC-PMIP} = \frac{1}{1 + \rho \sqrt{N}} \quad \text{if } t \leq T_{\text{FMC}}
\]
\[
\theta_{OF-FMC-PMIP} = 0 \quad \text{if } t > T_{\text{FMC}}
\]

6. RESULT ANALYSIS

All of the above discussed performance factor has been plotted to illustrate the improvement gained by implementing our approach OF-FMC-PMIP. Table II shows the system parameters that have been used where some of the parameters are taken from [14] and [15].
Concerning the tunnel usage in Figure 5, the variation of SMR shows that OF-FMC-PMIP and DP-PMIP are identical when $\leq T_{FMC}$ (before FMC session migration of CN) and present better tunnel usage comparing with I-PMIP. However, when $> T_{FMC}$ (after FMC session migration of CN) OF-FMC-PMIP becomes the best solution with 0% tunnel usage. This is due to the release of the tunnel between LMA1 and LMA2 after the CN migration in the cloud side (after $T_{FMC}$ delay).

Figure 4 shows the data delivery path length of the compared approaches. We can see clearly that the shortest data delivery path length is registered in intra-domain communication (16 hops) and this whatever is the approach. In inter-domain communication, the data delivery path length is longer (21 hops) this difference is due to tunnel use between LMA1 and LMA2 to forward traffic for/from MN in its new domain. If this is the case for I-PMIP and DP-PMIP approaches, the OF-FMC-PMIP in contrast, presents the advantage of returning to the same data delivery path length as an intra-domain communication (16 hops) after a $T_{FMC}$ delay (300ms).

Table 2 System parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>N</th>
<th>$d_{req}$</th>
<th>$d_1$</th>
<th>$d_2$</th>
<th>$d_3$</th>
<th>$\alpha$</th>
<th>$\tau$</th>
<th>$\delta$</th>
<th>$\beta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Values</td>
<td>32</td>
<td>1 hop</td>
<td>5 hop</td>
<td>5 hop</td>
<td>10 hops</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

For the illustration of signaling cost as a function of SMR (Figure 5), we can note that the signaling cost of OF-FMC-PMIP solution is relatively high compared to the other when $\rho$ is very close to zero (highly mobile regimes). This is evident from the fact that the IDMID must send an additional message (SESSION-MIGRATION-REQUEST) to the FMCC by each new inter-domain migration. The difference becomes less significant when $\rho$ increases.

Figure 6 illustrates the handover latency when SMR is varying and $t_d$ fixed to 100ms. We observe clearly that OF-FMC-PMIP and DP-PMIP are identical and offer better handover latency comparing to I-PMIP and more particularly when $\rho$ is very close to zero (highly mobile regimes).

Concerning the tunnel usage in Figure 5, the variation of SMR shows that OF-FMC-PMIP and DP-PMIP are identical when $\leq T_{FMC}$ (before FMC session migration of CN) and present better tunnel usage comparing with I-PMIP. However, when $> T_{FMC}$ (after FMC session migration of CN) OF-FMC-PMIP becomes the best solution with 0% tunnel usage. This is due to the release of the tunnel between LMA1 and LMA2 after the CN migration in the cloud side (after $T_{FMC}$ delay).

Figure 4 Data delivery path length between MN and CN

Figure 5 Tunnel usage variation with SMR ($\rho$)

7. CONCLUSION AND FUTURE WORK

The OF-FMC-PMIP framework introduced in this paper is a solution that permits to achieve the Follow Me Cloud concept, enabling thus mobile cloud services to follow their users according to their movements by migration services to the optimal datacenter and ensuring to them better Qos/QoE. The OF-FMC-PMIP combines the operator core network elements with those of the service provider network elements and this by implementing the following two parts: (1) Introducing a new inter-domain PMIPv6 mobility management support that relays and extends DP-PMIP solution and interacts with a system based on SDN/OpenFlow, to which users mobility information are pushed (2) The second part is an architecture based on SDN/OpenFlow, it exploits the mobility information delivered by the PMIPv6 inter-domain mobility management support and can trigger a seamless services/sessions migration in datacenter/cloud level in the goal of improving Qos/QoE of end-users.

A numerical analysis demonstrates that OF-FMC-PMIP in its PMIPv6 inter-domain mobility management support gives better performance compared to other solutions and more specifically in data delivery path length and tunnel usage. This is due to the fact that OF-FMC-PMIP permits to have a tunnel-free architecture after CN’s sessions/services migration, and the setup of direct routing by the FMCC OpenFlow Controller in the SDN architecture.

The scalability at the control-plane level (control flow) is the key factor to make the FMC based on SDN/OpenFlow usable in large scale networks. That is why we will focus on this aspect in the next works. Also, an implementing of the solution in a simulation test-bed will be made based on an open source PMIP and OpenFlow with the Network Simulator NS-3 to provide a near-to-real experiment of the approach.

REFERENCES


