Network Architectures for Ubiquitous Home Services

Warodom WERAPUN, Julien FASSON, Beatrice PAILLASSA

University of Toulouse, IRIT Laboratory, INP – ENSEEIHT

email: {warodom.werapun, beatrice.paillassa, julien.fasson}@enseeiht.fr

***Abstract*— The on-going growth of connectivity has brought new opportunities for Home Network; Home network will soon be a place of a large amount of services, from the gadget to the home control. In order to provide and render these services, operator should propose a framework for supporting the deployment of new services. This paper focuses on home services, proposing an overview of potential service architectures. Then a photo sharing services validates through implementation the concepts of Home Services and an analysis of architecture complexity is proposed to conclude this work.**

***Keywords*— home network, network architecture, home services, P2P, IMS, SIP.**

I. Introduction

With the rapid growth of the Internet, more and more users have an Internet access at home. This connectivity is rendered by a set top box proposing a set of services. However, most of these services are simple and static (mainly triple play) and are only managed by the network operator.

In the same time, web evolution has lead to miscellaneous services like photo sharing (picasaweb), video sharing services (youtube), social networks (facebook), etc. Such services offer more interactivity and can be directly managed by users. Nevertheless, in some cases service providers become owner of personnel data, inducing an issue of privacy for user and an issue of content right for providers. Also, the management by operator of home service enabling a local management and storage of service content solves the issue of privacy that user encounters with web services. Indeed service providers become owner of any piece of information you share through the service. Home service may also simplify the issue of copyright that provider encounters with illegal piece of information. However the responsibility of service provider may be engaged depending on way of referencing the content, as for the P2P trackers for bittorrent.

The challenge is to merge the dynamic web services at the set top box so as to propose a direct management of their services to users through their home network. As we aim at integrating service at home, we need a suitable network architecture to support service deployment and data flow.

This paper introduces home network concept, their services and their needs. Then convenient network architectures for home services are proposed. A simple service is implemented to illustrate our deployment of home services. Eventually an analysis of network architectures concludes this paper.

II. Home network and services

A. Context

Home Network (HN) is a small network which connects all home terminal devices together (Figure 1). Deploying services between on the HN will bring a lot of possibilities and new service uses (e.g., view photos from mobile phone on a large television screen; remotely control an air condition from any ubiquitous terminal devices, etc.). Since through the HN a user can access private resources and command all connected terminal devices remotely, the network must be secure.

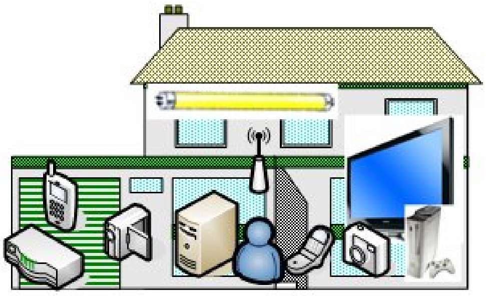


Figure 1: Home network example

Home Services (HS) are a set of miscellaneous ubiquitous services that operate at home. A same user may access to his services through miscellaneous types of access networks from a lot of devices, especially with the growth of portable technologies. In addition, these ubiquitous home services can be deployed from home by a network operator or directly by user. They can be controlled both locally and remotely. (e.g., change radio channel from personnel computer at home, check refrigerator information from mobile home remotely).

There are different types of HS. A HS can be static or dynamic. A static service is managed by the operator (e.g., TV service) and home user can just use it since they are installed by the network operator. Dynamic services are controlled services that the service owner is able to manage or change without interrupting the system (e.g., multimedia sharing service). Finally HS may be intra-home service, home to home services or community ones.

B. Needs

Supporting Home Services requires allowing users to remotely connect to their HN. HS are dealing with many home equipment devices which suppose to be acquiring, viewing and managing digital content with any ubiquitous devices from any location. Personal home content and control need privacy and rightful access. These conditions raise the need of security. Moreover in order to offer home to home services like content based services, HN must be able to connect to other HN though their home gateway. As a result, HS and HN must have effective authentication and authorization mechanisms.

Since lots of HSs are expected to be deployed, they should be developer-friendly while their exchanges, their installations and their uses should be easy between HNs.

Finally, as resources and services are numerous, they induce a lot of content to share. To locate the data and/or resources it needs a service of indexation. The service of indexation directly impacts the service architectures. In this work two kinds of management are considered:

- The centralized service index: located on one single server. User can search the service or data by requesting the central index server and then go directly to service or data owner at his home.
- The distributed service index: divided in several parts. Each part is located in one or several servers. Users can search the service or data by asking index servers that depends on searching algorithm and then go directly to service or data owner at his home.

III. PROPOSITION OF NETWORK ARCHITECTURES FOR HOME SERVICES

A. Main Architectures

The object of network architecture is to delivery home services to users. As the users may be local, remote or visitor, the architecture has to manage (as transparently as possible) user accesses to their home services. Furthermore, by considering the community framework, the architecture must in addition manage the user data localization.

Basically of achieve service architectures, there are IMS (IP Multimedia Subsystem) [1], P2P (Peer to Peer) [2], VPN (Virtual Private Network) [3] and Web architecture.

IMS is defined as an architectural framework created for the purpose of delivering IP multimedia services to end-users. It supports IP Multimedia sessions, quality of service (QoS) requirement, interworking with the Internet and the circuit switched network, roaming as well as the ability for operators to have a strong control on the services of users. IMS uses SIP (Session Initiation Protocol) [4] as signaling. SIP is the text based signalling protocol to sets up multimedia sessions between endpoints. These sessions may be text, game, voice, video or a combination of these. It is a centralized scheme as the services and users are managed by a central functional entity.

P2P is a relation of connected devices which have equivalent privileges and which share their resources and services together. It is a distributed architecture. In addition, there are several types of P2P such as pure P2P, hybrid P2P and DHT P2P [5] etc.

VPN provides the secure tunneling to establish sessions. There are a lot of interconnecting scenarios in case of using the VPN technology. Users can directly make a VPN tunnel to a server with their home gateways. This aims indeed to create a connection with a VPN server that is able to access to the gateway for achieving services or resources as previously described since some services have policies that clients have to stay in the same network with the server.

Concerning web architecture, it is a client-server based. All data and indexes are stored at one central server. All users achieve them from a central web server.

The choice of an architecture is depended on many factors, especially the performance, the security and the scalability. For a global point of view, considering the performance aspect and scalability aspects, centralized architecture, as IMS, seems to be adapted to home to home service, while distributed P2P technique would be convenient for community services. On the contrary, when tacking account the security aspect, centralized architecture seems preferable whatever the type of service.

Next paragraph details more precisely IMS and P2P architecture on a service example.

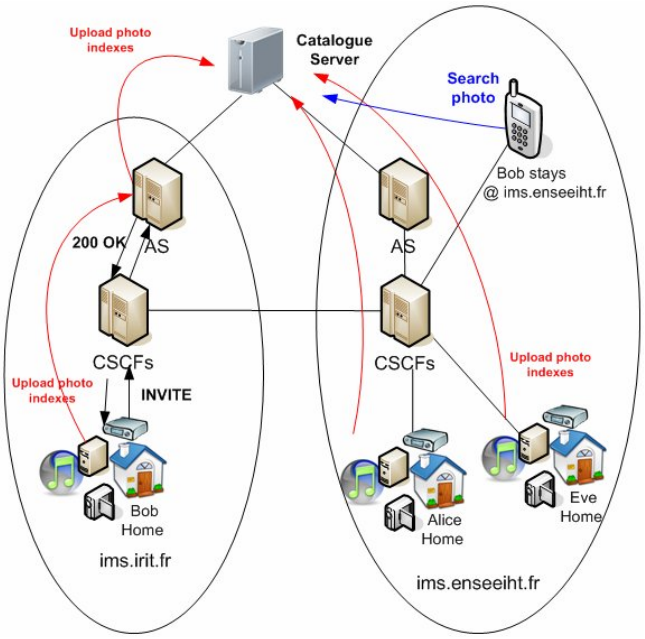


Figure 2 : Photo sharing with IMS Architecture

B. IMS Architecture

The architecture is illustrated on a service scenario. The service is a photo sharing service with a central catalogue server on IMS architecture. The catalogue server is defined to manage resource addresses which are published by clients.

IMS scenario: In Figure 2, Bob, with his home network, registers himself at ims.irit.fr domain. Alice and Eve stay at ims.enseeiht.fr domain. They can upload their photo lists to the catalogue server. The catalogue server is attached with the Application Server (AS). AS is connected with Call Session Control Functions (CSCFs) and it will be trigged by matching the IMS signalling which is defined in Home Subscribe Server (HSS). When Bob stays outside his home, if he would like to search some photos, he just looks in the catalogue server to acquire preferred photo addresses via CSCFs. Then, he can directly download from his friends following retrieved addresses. CSCFs will responsible for session establishment which includes authentication and authorization to the catalogue server.

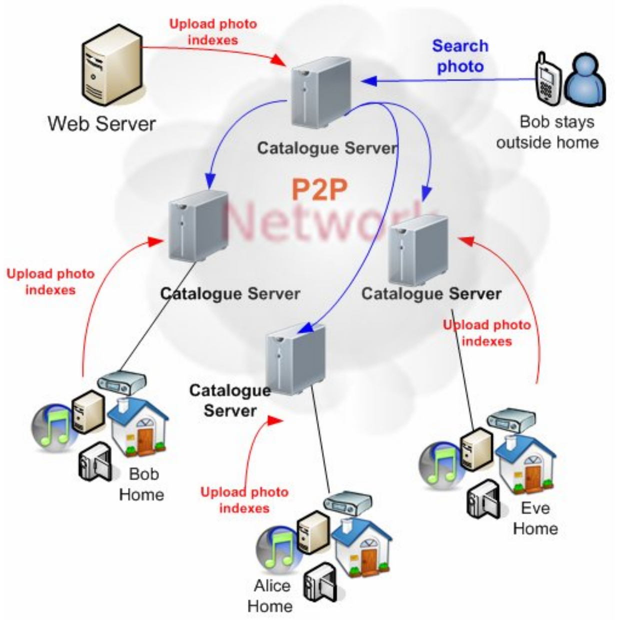


Figure 3: Photo sharing with P2P Architecture

IMS security aspect: IMS standard proposes a security architecture that uses several security protocols such as IMS Authentication Key Agreement (AKA) [6] between User Equipment (UE) and IMS network via P-CSCF, IP Security (IP Sec) [7] between UE and P-CSCF, Diameter [8] between HSS and I/S-CSCF. IMS uses AKA for authentication and IPSec for confidential and integrity. IMS provides strong security mechanisms that suppose to be efficiently secured the platform. Unfortunately, most of the real deployment is not rigorously clung all IMS security standards, e.g., some ubiquitous devices do not support IPv6 and/or IPSec as mandatory in IPv6 [9]. Moreover, only a few IP phones supported AKA. Due to lack of an IMS Subscriber Identity Module (ISIM) in laptops, they use MD5 digestion authentication instead. In addition, because of IMS security architecture implementation is truly complex. As a result, it had led to simplify security mechanism and they also lead to vulnerabilities.

C. Centralized P2P Architecture

The P2P network considered is a centralized P2P. As in IMS, signaling may also be SIP [9].

P2P scenario: The photos sharing service scenario is quite similar to the IMS architecture. There are publishing, searching and retrieving. IMS takes all indexes into a single central catalogue server; instead P2P divides indexes in to several parts and leaves them to several catalogue servers as described in Figure 3. Connected user in the network can share by upload the photo indexes to a catalogue server. Then, another user (e.g., Bob) can search and directly download the photo that he wants from the photo owner.

Centralized P2P security aspect: Many kinds of security architectures that are depended on the efficiency level of protection can be integrated. For minimum level, it can be assumed that all peers are trusted. To increase security, mechanisms can be added as a centralized AAA server, Kerberos [11], a server for generating session tickets to clients, proxy server authentication, peer signatures in the centralized P2P and public/private key cryptography. In addition, it could be used with the challenge/response protocol to authenticate each others. However, lots of certify mechanisms lead to decrease system performances. This should be considered before to decide to apply the security mechanism.

IV. EXPERIMENTAL

Java and JAIN-SIP [12] library have been used to implement the photo sharing service on P2P network architecture with SIP signalling. It consists of 3 phases: publishing, searching and retrieving.

The main components of the service (Figure 4) are:

- Global/local manager: manage contact list for server/client
- Contact List: friend address list, Data & Index: resource addresses
- SIP UA (User Agent). SIP UA is used to be SIP interfaces to other users. It is used to establish the session for specified applications.

Peer stores its data and indexes. Peer publishes its sharing indexes to the catalogue manager. Catalogue manager maintains sharing indexes. Contact list stores a list of peer's friends which is managed by local manager.

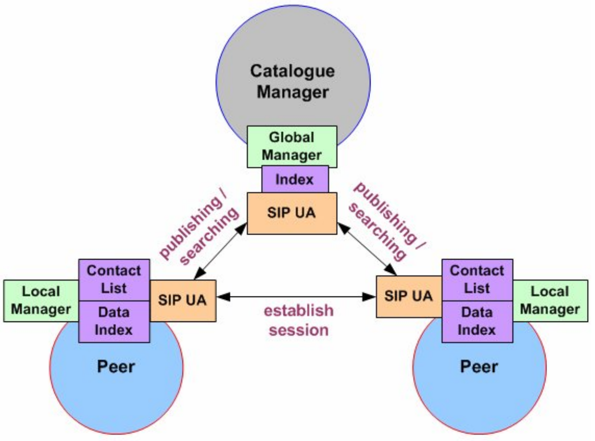
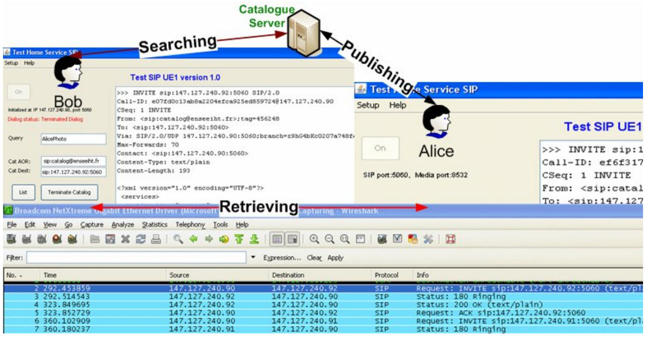


Figure 4: Photo sharing design component


Catalogue Server
Searching
Publishing
Retrieving
Test Home Service SIP
Setup Help
On
Bob
Test SIP Service SIP
Setup Help
On
Alice
Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft) Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

Test SIP UE1 version 1.0

Initialized at IP 147.127.240.90, port 5060

Dialog status: Terminated Dialog

Query: AlicePhoto

Cat AOR: sip:catalog@enseeiht.fr

Cat Dest: sip:147.127.240.92:5060

List | Terminate Catalog

```
>>> INVITE sip:147.127.240.92:5060 SIP/2.0
Call-ID: e07fd0c13ab8a2204efca925ed859724@147.127.240.90
CSeq: 1 INVITE
From: <sip:catalog@enseeiht.fr>;tag=456248
To: <sip:147.127.240.92:5060>
Via: SIP/2.0/UDP 147.127.240.90:5060;branch=z9hG4bKc0207a748f
Max-Forwards: 70
Contact: <sip:147.127.240.90:5060>
Content-Type: text/plain
Content-Length: 193

<?xml version="1.0" encoding="UTF-8"?>
 <services>
```

Test SIP UE1

SIP port:5060, Media port:8532

```
>>> INVITE sip:1
Call-ID: ef6f317
CSeq: 1 INVITE
From: <sip:catal
To: <sip:147.127
```

```
No. .  Time         Source           Destination      Protocol  Info
     2 292.453859   147.127.240.90   147.127.240.92   SIP       Request: INVITE sip:147.127.240.92:5060 (text/pl
     3 292.514543   147.127.240.92   147.127.240.90   SIP       Status: 180 Ringing
     4 323.849695   147.127.240.92   147.127.240.90   SIP       Status: 200 OK (text/plain)
     5 323.852729   147.127.240.90   147.127.240.92   SIP       Request: ACK sip:147.127.240.92:5060
     6 360.102909   147.127.240.90   147.127.240.91   SIP       Request: INVITE sip:147.127.240.91:5060 (text/pl
     7 360.180237   147.127.240.91   147.127.240.90   SIP       Status: 180 Ringing
```

Figure 5: Photo sharing screenshot

Figure 5 shows the implementation screenshot. This application is based on a SIP signalling to communicate with the connected users for session establishment following SIP standard. The specific service communication protocol (e.g., photo sharing service) is defined by attaching xml elements with the SIP body message (MIME type) [13] in text/plain format. Moreover, service communication protocol is mapped with the POJO (Plain Old Java Object) for easier managing. We had tested that our application can established SIP session with the catalogue server and can directly share photo between friends successfully.

V. Analysis and Comparison

The study focuses on the signaling induced by registration, publishing and retrieving, for different architecture and security mechanisms.

A. Client signalling

A first point is to analyze client signalling: counting the procedure weight by number of messages (e.g., sending and receiving by the UE) and the size of these messages. Because the kind of messages is the same, counting them is sufficient.

Let analyze in the client side of the IMS and the SIP central architectures as indicated in Figure 6. There are IMS Client, SIP Client1, SIP Client2 and SIP Client3. IMS Client is an IMS UE that works following IMS standard. The SIP clients differ from their authentication mechanisms. More precisely, when IMS client is connected with different network operators, IPSec session is used to secure the communication (it could be both transport or tunnel mode), however, SIP clients are free to define security protocol, and then it can be applied with lighter security (SIP Client1) until stronger security (SIP Client3) .

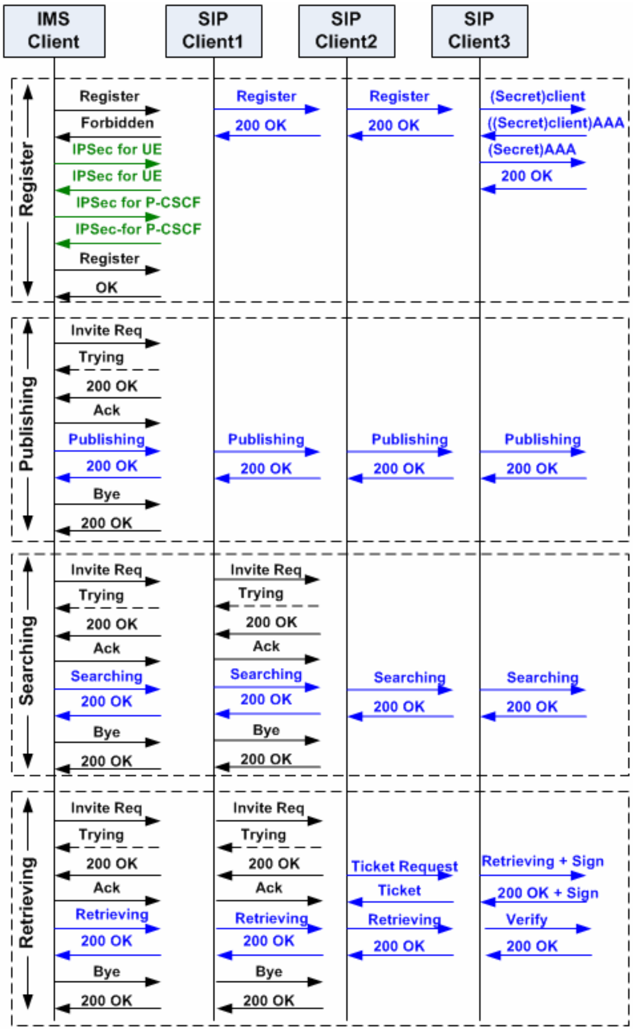


Figure 6: Client signalling

About the signalling is presented in the Figure 6. It is connected to the way to manage content sharing with SIP. A first solution is to have sessions with the catalogue for publishing and searching, and a session with the sharing client for retrieving (as illustrated in Figure 6 with SIP client 1). In this case, the client signalling is similar to the IMS case except the authentication part. However, we can define specific SIP signalling at least for publishing and searching that does not require a session (as indicated in Figure 6 with SIP client 2 and 3).

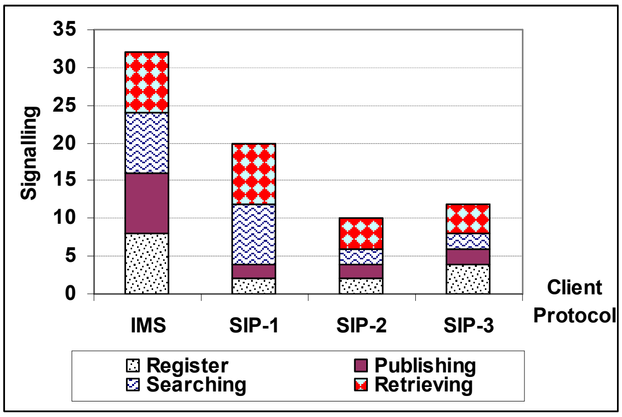


Figure 7: All client signalling summary

Figure 7 shows summary of client exchange signalling for each phases and theirs total. We can see that IMS client handles more procedures than SIP clients. However, IMS solution might be optimized because its standard includes a lot of SIP signalling. In addition, it also proposes a native security mechanism. For the application signalling, photo sharing service needs 2 signalling (request/response), SIP-2 and SIP-3 embed an application query in SIP signalling. This analysis can be extended to any kind of services that have request/response flow like the photo sharing one.

B. Signalling summary

The first evaluation gives a global point of view on the client side but it does not reveal the complexity of the whole architecture. The second point is to evaluate the overhead of signalling over the whole architectures. Thus, counting exchanged messages between all nodes allows us to have an overview of global behaviour.

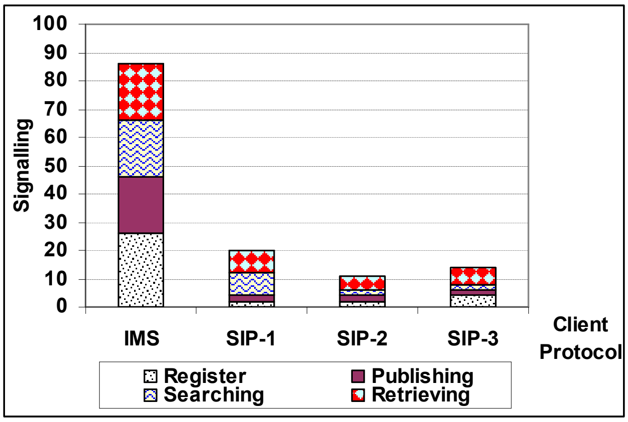


Figure 8: Whole signalling in all network architectures for one searching

Figure 8 shows whole signalling in all considered network architectures for one searching. It focuses on all signalling that is related to a downloader who tries to get the content from a sharer.

IMS has lots of signalling because its standard requires several components (e.g., CSCFs, HSS and ASs) to create and establish the session. In contrast, centralized SIP has defined only a centralized index component. Then, we can build the system with our preferred security mechanism which depends on the required security level and the system performance.

In SIP cases, we propose: 1) Password authentication (SIP-1): login one time to the network, 2) Kerberos ticket (SIP-2): use Kerberos server to issue ticket for communicating between peers, and 3) signature authentication (SIP-3): peers have to sign all signalling and verify with the authentication server. In the fact, there are more security mechanisms which are possible to use. However, these solutions induce different security levels and network performance.

IMS is greedier signalling mainly in whole architecture. It needs an infrastructure, processes in each entity and very complex in the register phase. Register phase is occurred when users firstly connect to the system or move to another location. However, searching and retrieving are considered to be frequently occurred than register phase. These are more dynamic and significant signalling to consider.

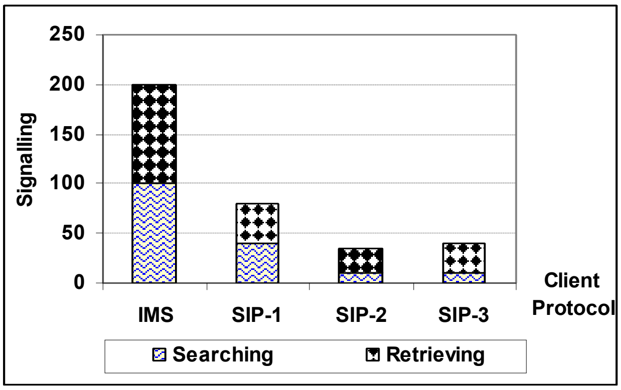


Figure 9: Signalling summary for five searching and retrieving

Figure 9 shows signalling summary for five searching and retrieving. We can see that SIP-3 still has less signalling than standard IMS. Moreover, when we try to increase searching times, the downloader searches the content in the network, signalling in IMS and SIP plus security are increasing undoubtedly. On the other hand, the ratio is decreasing since the major difference is occurred at registration phase. Moreover, when we added security mechanism to SIP central architecture, signalling is increasing. This will lead to decrease network performance. However, it has to consider by the system manager that how much for the system security is required with this tread-off.

VI. CONCLUSION AND FUTURE WORKS

In this work, we presented home services and network architectures for the future delivery of dynamic services to home users. Next, we propose service classification, and network architectures for home services. Based on existing SIP protocol and IMS architecture, this paper exposes a new SIP based framework with security that is compared with IMS solution. We show exchanging message comparison between IMS and centralized SIP architectures with interested security mechanisms and we can see that IMS architecture is more complicated than centralized SIP.

As we previously described for the SIP matter, we have to add security protocol, authenticate and authorize users each time with all peers that they are connected, client application needs to aware security with the SIP application server. In addition, to integrate security protocol in P2P is also interesting since P2P gives more benefit e.g., scalability and availability but it also creates more overhead and complexity especially in security management.

We will attempt to focus more precisely in community networks to do service sharing and build the system by using several P2P architectures (e.g., hybrid P2P, DHT P2P). This study is our future step towards numerous works. A first element might be a real implementation of sharing services. This implementation could be deployed on different types of P2P architectures so as to compare their performances, their relevance and their security aspects. Other services could also be deployed on the more relevant architecture. Finally, the IMS architecture could also provide a support to P2P services. A coupling of these 2 architectures might be an interesting study too.

ACKNOWLEDGMENT

The research is supported by European Celtic Project under Feel@Home project.

REFERENCES

[1] 3GPP, "IP Multimedia Subsystem (IMS)," TS 23.228, Release 8, Version 8.7.0, Dec 08

[2] G. Camarillo, Peer-to-Peer (P2P) Architecture: Definition, Taxonomies, Examples, and Applicability, RFC 5694, IETF Network Working Group, Nov 2009

[3] E. Rosen and Y. Rekhter, BGP/MPLS VPNs, RFC 2547, IETF Network Working Group, July 1999

[4] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler, SIP: Session Initiation Protocol, RFC 3261, IETF Network Working Group, 2002

[5] I. Stoica, R. Morris, D. Liben-Nowell, D. R. Karger, M. F. Kaashoek, F. Dabek, and H. Balakrishnan, Chord: A Scalable Peer-to-Peer Lookup Protocol for Internet Applications, IEEE/ACM Transactions on Networking, Vol 11, Feb 2003

[6] A. Niemi, J. Arkko and V. Torvine, Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA), RFC 3310, Sep 2002

[7] S. Kent and R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, IETF Network Working Group, Nov 1998

[8] P. Calhoun, J. Loughney, G. Zorn and J. Arkko, Diameter Base Protocol, RFC 3588, IETF Network Working Group, Sep 2003

[9] Frank S. Park, Devdutt Patnaik, Chaitrali Amrutkar, Michael T. Hunter, A Security Evaluation of IMS Deployments, IMSAA 08, Dec 2008

[10] C. Jennings, B. Lowekamp, E. Rescorla, S. Baset and H. Schulzrinne, REsource LOcation And Discovery (RELOAD) Base Protocol, draft-ietf-p2psip-base-08, Mar 2010

[11] C. Neuman, T. Yu, S. Hartman and K. Raeburn, The Kerberos Network Authentication Service (V5), RFC 4120, IETF Network Working Group, July 2005

[12] JAIN-SIP Developer Tool, https://jain-sip.dev.java.net/ (Accessed: 4 June 2010)

[13] N. Freed and N. Borenstein, Multipurpose Internet Mail Extensions, RFC 2045, IETF Network Working Group, Nov 1996