Convergence architecture for home service communities

Warodom Werapun, Julien Fasson, Béatrice Paillassa

Convergence Architecture for Home Service Communities

Warodom Werapun[*1], Julien Fasson[2], Beatrice Paillassa[3]

[*1]Department of Computer Engineering, Faculty of Engineering, Prince of Songkla University, Thailand
[2 3]University of Toulouse, IRIT Laboratory, INP-ENSEEIHT, Toulouse, France

[*1]warodom@coe.psu.ac.th; [2]julien.fasson@enseeiht.fr; [3]beatrice.paillassa@enseeiht.fr

Abstract

Nowadays, home networks have integrated day to day life through the classical internet access and deliver numerous services to end users. This home entrance is a real opportunity for operators to deploy services directly between homes. However, one major issue is the interconnection between Home Networks (HN) which requires suitable architectures and efficient authentication mechanisms. In this paper, two network architectures were proposed to interconnect HNs in order to support home service delivery and then compared with the IMS as reference architecture. The first architecture was based on a centralized SIP solution and used HTTP digest for authentication purpose; while the second proposition consisted in a distributed architecture based on pure P2P and Identity based cryptography. The study of these two solutions has been undergone through the simulation of a simple photo sharing scenario. As a result, the centralized SIP solution can be relevant for an average number of users and the easiest way to deploy new services. The decentralized solution (pure P2P) can be deployed for small service communities and may be compliant to larger system with improved algorithms.

Keywords

Authentication; Network Architecture; Home Services; P2P; IMS; SIP, Content Network

Introduction

Convergence architectures are elaborated to support multiples services over multiple networks and technologies. According to this concept, operators of ITU networks are elaborating the Next Generation Networks. The basics are to use packet networks to transport services in a common way with various data of services and to offer an integrated level for the management of services (i.e. user profile, authentication, etc.) whatever the access used is. The paper focuses on the service convergence aspectby studying IMS architecture in order to deliver services at home users, in which two alternatives architectures have been proposed.

In the past, network operators handled services with dedicated architectures as voice with the PSTN and Internet data with ADSL. Nowadays, especially when considering the explosion of smartphones, services are more concerned about content delivery. The objective is to establish contact not only between users (e.g. telephone, video conference) but also between a user and content including data, voice, video and any combination of them. Content delivery architectures are proposed by service operators over Internet (i.e. Akamai) through the networks of other operators. In this study, our objective is to study a service delivery architecture that would be directly proposed by a network operator to its users, at their homes. While content services are already available, the originality of this work is to consider them not in the "Internet space" but in the home and operator domains. Data are owned by users at home and their sharing is orchestrated by the network operator.

Users are able to share content among a community, through a home gateway (operator box). The resource location (named index management in the paper) could have been managed as it pleases. However, to deploy such services without a too fussy application control part, a global management of access rights is needed: resource indexation, or at least community management, should be proposed by the global architecture.

Various network operator architectures can be deployed. In this paper, two solutions were presented, P2P and SIP, and their advantages and inconveniences were studied. The first part of the paper determined the main exchanges for the given scenario on a pure P2P architecture and on a SIP based centralized solution. Then, authentication mechanisms are analysed. From this analysis, modelling and evaluation of architectures were conducted. In the last part, the propositions were compared to the actual service architecture of the operators: IMS.

Content Service Architectures

Types of Architectures

Two kinds of solution were studied to deploy the service depending upon the service usage that may be low or important. There are pure P2P [RFC 5694] which stands for original Internet design where end-to-end paradigm is respected, and Session Initiation Protocol (SIP) [RFC 3261] solution which is based on a network paradigm with some centralisation.

Since in a first step small communities has been taken into account, pure P2P architectures with its ease to deploy services may offer a relevant solution. However, centralized solution can also be considered because they are more compliant to the operator point of view. Centralized SIP seems an unavoidable proposition and will be compared with pure P2P

This work utilized a simple content delivery service, photo sharing, as a sample reference scenario to analyse and compare network architectures. In this scenario, Alice shares a photo with Bob.

Three parts are considered for the service. There are:

- Publishing, the sharer maintains resource indexes to downloaders.
- Searching, the downloader lookups resource addresses.
- Retrieving, the downloader gets resources from sharers at the addresses obtained during the Searching step.

Next section detailed the main steps of the scenario for each architecture.

Scenario in Decentralized Pure P2P

In pure P2P, each peer directly keeps the index of their own resources. Thus there is no publishing step. Bob looks for a photo by selecting keywords and flooding them to its neighbours (searching). All peers forward his request until there is a match with local index or until the applicative Time-To-Live (TTL) is reached (e.g., 4 hops for default configuration in a typical Gnutella client). Each matching node answers Bob. Finally, he can select the relevant photo and download it directly (retrieving).

Scenario in Centralized SIP based

In the centralized solution, Alice publishes her resource indexes to the catalogue server (publishing), while Bob sends his searching query to the catalogue server. This one answers Bob that Alice has a matching photo (more than one searching result can be returned). Bob can select the most relevant answers before starting to download it (retrieving).

For publishing and searching data, SIP PUBLISH and OPTIONS were selected, respectively. Retrieving was done by using SIP INVITE.

Authentication Aspects

Authentication mechanisms were detailed along the photo sharing scenario so that signalling exchanges will be evaluated.

Identity based Cryptography in Pure P2P Solution

P2P architectures for resource sharing did not initially provide strong authentication mechanisms. However, the global need of security in the Internet has brought authentication mechanisms to P2P. The challenges are: eliminated certificate server, inside intruder and management cost etc. There are many existing solutions like Web of Trust using Pretty Good Privacy (P. Zimmermann, 1995), Distributed authentication and Byzantine fault tolerance (V. Pathak, 2006), and trusted score mechanisms (Y. Zhang, 2009).

In an HN context, the situation may be a bit different since home gateway could be configured by the operator. It is proposed in this study then to use the Identity Based Cryptography (IBC) (A. Shamir, 1985) to avoid issues related to validation; in which the user's identity (ID) was taken as a public key and so eliminating the need of a certificate server. IBC is based on the elliptic curve encryption, an asymmetric cryptography that offers many advantages in terms of performance and deployment for distributed environment (I. Blake, 2005).

There has a trusted key generator centre (PKG), whose task is to set up the whole system parameters and to extract all user private keys based on user identity and system parameters. After Bob and Alice obtained their private keys and system parameters from PKG, Bob applied Alice's ID as her public key to encrypt his message and sent it to her. Bob did not need to verify Alice's public key since Alice ID is never bogus. Alice can decrypt Bob's message using her private key. Note that ID may be associated to an expiration date for key revocation purposes (e.g., alice@example.com|12mar 2012). In this case, PKG needs to check that there is no user with duplicated ID and different expired dates to prevent ID impersonation. Revocation cost is not more than traditional public key cryptography and gets advantages in the certificateless. It was assumed that

there is not any malicious action during this phase since the goal of this study is to evaluate signaling. Degree of protection can be considered in other research topics.

The precise signaling exchanges are:

Registration phase: Bob, the Source Node (SN), connects to the P2P networks using any kind of bootstrap information to the bootstrap node(s) with its signature and encrypts it with the identity. Each future neighbor decrypts the message and verifies the SN signature. Then a register result is sent back that is signed by its signature and encrypted by the SN Identity. Two signaling messages per neighbor have been exchanged.

Searching phase: SN floods a searching query with its signature to its neighbors. They forward the message according to the specific time-to-live (TTL) value.

Retrieving phase: Once SN found content at Correspondent Node (CN),its ID is taken as a public key to sign and encrypt data that will be sent to CN. SN sends retrieve request. CN returns a retrieve result with session key and its signature. This message is encrypted by SN Identity. SN verifies the message and sends back ACK message to CN. SN sends OPEN to request sharing resource which can also be encrypted with the previously session key. CN responds ACK to SN and session is established. After that session is terminated by sending CLOSE and waiting ACK, the number of signaling messages is 7.

HTTP digest in Centralized SIP based Solution

Many solutions have been proposed to add authentication (W. Werapun, 2009). With the help of SIP proxies, users are able to be more secure by introducing some filtering and also dividing verification tasks from a centralized server. Besides, it is proposed to use HTTP digest (J. Franks, 1999) with pre-share secret key for authentication since it is simple, can be deployed with a centralize AAA server with proxies, and outperforms asymmetric key and is already supported by SIP. HTTP digest is an acceptable method where users negotiate credentials with a server. Pre-shared password is digested with some related text before being sent on the network to authenticated users. The algorithm for HTTP digest authentication is MD5.

Illustration of this solution is shown in Fig. 1. Pre-shared key between all users and AAA is required and links between proxies and AAA are secure tunnel. This assumption is reasonable since all proxies are usually fixed.

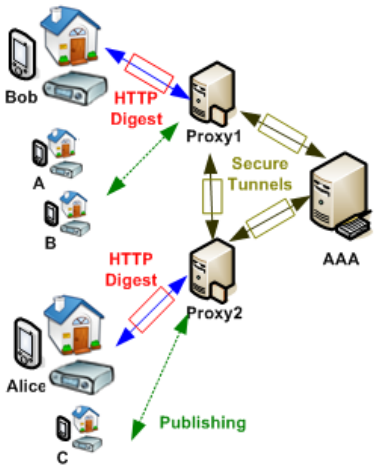

FIG. 1 SIP BASED AUTHENTICATION

The main steps of this authentication are:

Registration phase: All communications are done via Proxy. SN sends a SIP register to AAA server as shown in Fig. 2. AAA server returns 401-Unauthentication to SN that then uses its pre-shared key and the previous parameters (nonce) from server to generate authentication information and returns to AAA a Register-AuthInfo. AAA server verifies the returned authentication information and sends back SIP 200 OK with parameters for a session key generation and a session key. The proxy removes the session key from the message and forwards the 200 OK with only the session key parameters. Finally, SN generates session key from received parameters with pre-shared key and starts to create secure tunnel with proxy by using this session key. There are 4 messages exchanged between SN and Proxy and 4 messages between Proxy and AAA.

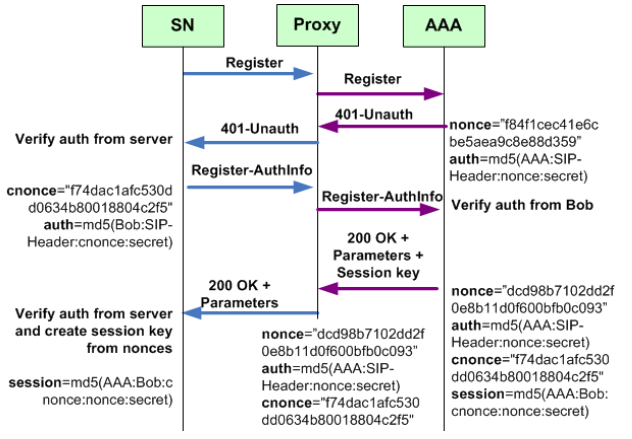

FIG. 2 HTTP DIGEST WITH SIP REGISTRATION

Publishing phase: CN publishes its resource indexes to a catalogue server (Cat) via its proxy server (Proxy). Indexes are embedded in SIP PUBLISH. Cat replies

with a 200 OK message. There are 2 messages from CN to Proxy and 2 messages between Proxy and Cat.

Searching phase: SIP OPTIONS is used as querying information from nodes. SN searches indexes from Cat by sending SIP OPTIONS including its keywords. Searching results are embedded in SIP 200 OK. 2 messages are exchanged between SN and Proxy and 2 between Proxy and Cat.

Retrieving phase: SN opens a session with the resource owner by sending a SIP INVITE with application specific query (e.g., photo URI). This invitation passes through its proxy and the CN proxy. CN returns 200 OK to SN that then sends back ACK to CN. Then, it downloads content directly and tears down the session by sending BYE and receiving OK. 5 messages are exchanged.

Modelling and Evaluation

In this part, the signalling cost of architecture, eventually compare the solutions was firstly analyzed.

Evaluation Reference: IMS Architecture

IP Multimedia Subsystem (IMS) (3GPP, 2003) is an operator view of service architecture which can provide strong security mechanisms. Therefore, it was considered as an architecture reference. IMS uses a long-term sharing secret key which is embedded in ISIM (IMS Subscribe Identity Module) to establish a secure channel. This process, called Authentication and Key Agreement (AKA) is based on HTTP digest authentication [RFC 3310]. The security parameters are generated during AKA process for having a session key used to secure communication channels.

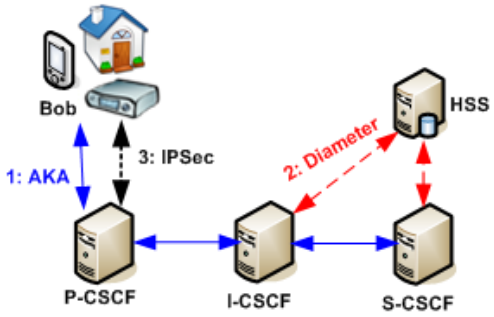

FIG. 3 IMS AKA

The main IMS entities are presented in Fig. 3. There are three types of Call Session Control Function (CSCF): Proxy (P-CSCF), Interrogating (I-CSCF) and Server (S-CSCF). Home Subscriber Server (HSS) is the client database.

Bob sends SIP REGISTER to its P-CSCF which acts as an outbound/inbound SIP proxy server for the IMS terminal (arrow 1: AKA). It communicates with DNS (Domain Name Server) to resolve SIP server domain. Then, P-CSCF forwards the I-CSCF. This one searches Bob's corresponding S-CSCF from HSS. Then, it forwards the REGISTER message to this S-CSCF. Communications between CSCFs and HSS use Diameter protocol. S-CSCF asks an authentication vector from HSS and challenges Bob through I-CSCF and P-CSCF consequently. If successful, Bob uses authentication parameters to establish IPSec [RFC 2401] with P-CSCF (arrow 3: IPSec). Once the two pairs of IPsec ESP Security Associations (SAs) have been done, the traffic is sent through the encrypted tunnel and P-CSCF will identify all the SIP requests coming through the corresponding SA as pertaining to the authenticated user. Thus, no more user authentication is needed. SIP signaling is clearly sent in the encrypted tunnel.

Signaling evaluation is summarized for the different steps:

Registration phase: Fig. 4 (left) shows registration signaling, and there are 3 parts: create credential (with SIP REGISTER and some diameter protocol with HSS), IPSec setup and challenge.

Publishing/Searching phase: Fig. 4 (right) shows publishing (or searching) signaling. There is always SIP INVITE to open a session. Note that publishing and searching have the same signaling in IMS.

Retrieving phase: Fig. 5 shows retrieving signaling. SN creates a session with CN using SIP INVITE. After a session is established, SN sends retrieving query through CN via IMS elements. Data is transferred from CN to SN. SN tears down a session.

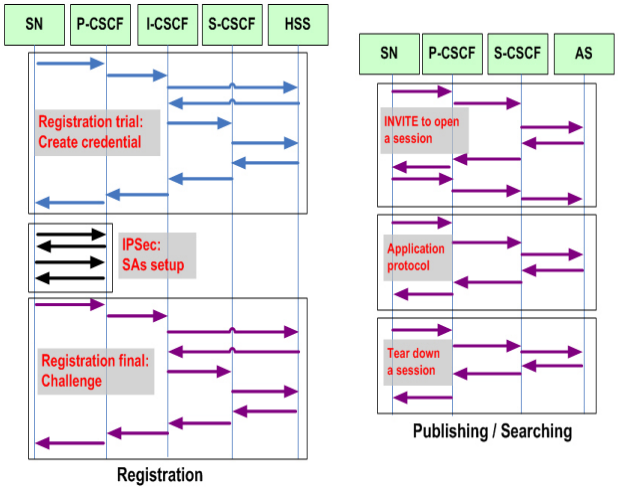

FIG. 4 IMS REGISTRATION AND PUBLISHING/SEARCHING SIGNALING

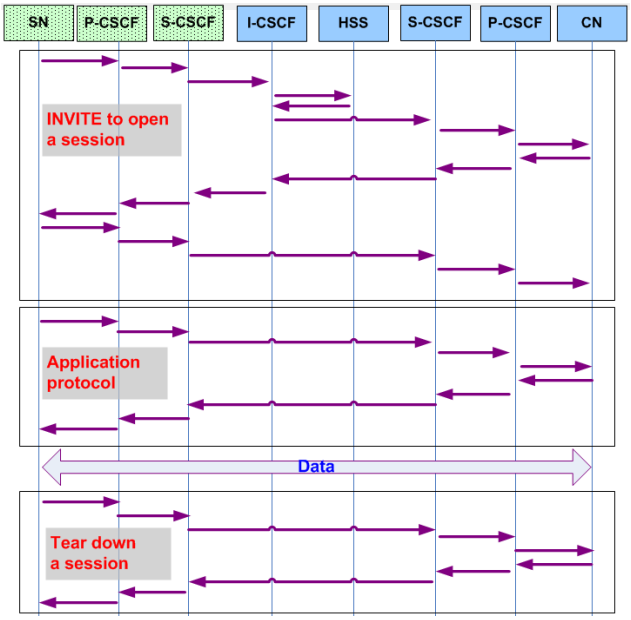

FIG. 5 IMS RETRIEVING SIGNALING

Topology Modeling and Signaling Cost Analysis

Considering the searching phase, the signaling in centralized solution does not depend on number of users whereas the pure P2P solution does. Thus, the first step of the study consists in analyzing pure P2P topology.

1) Topology Modelling and Evaluation

Characteristics of P2P model are the number of nodes and the interconnections distribution. In pure P2P overlay, the distribution of node degrees may be modeled from a power law (M. Jovanovic, 2001). A number of real-life P2P networks have compliant topologies with this distribution (M. Jovanovic, 2001). When a node *i* joins the network, the probability that it connects to a node *j* already belonging to the network is given in (1), where *d* is the degree of the target node, *V* is the set of nodes that have joined the network and $\sum_{k \in V} d_k$ is the sum of degrees of all nodes that have previously joined the network.

$$P(i,j) = \frac{d_j}{\sum_{k \in V} d_k} \quad (1)$$

The size of physical network is assumed to be 1,000 connected nodes (home gateways and routers) and the size of participated users is 100 connected users. Pure P2P topology is generated by using BRITE (A. Medina, 2001) tool with Barabasi-Albert model (A. Barabasi, 1999)which creates a graph having 1,000 nodes for the physical network and *n* nodes for an overlay network following the power law distribution. From this physical network, 100 overlay topologies with minimum degree equal to 1 and 100 others with minimum degree equal to 2 are generated per each value of *n*. These nodes are randomly selected among the nodes of degree 1 of the physical network.

The flooding signaling and the average hop distance have been evaluated. For the flooding TTL has been valuated to be 4 as default configuration of typical Gnutella client. An average search signaling was computed by testing communication among all nodes (changing source and destination nodes until reaching all nodes). As a result, S_n^{cost} values were obtained which are denoted as the signaling searching cost for *n* connected nodes in the overlay network (*n* varying from 10 to 100 and increase 10 nodes for each step). Concerning the hop distance, senders and receivers have been randomly selected in the simulated overlay network, then routing based on Dijkstra algorithm is applied resulting in an average hop distance between SN and CN of 7.

2) Signaling Cost Analysis

The cost considers the number of signaling exchange, expressed in the previous section and the distance between the source and the destination of the exchange. A distance of *n* induces n transmission cost in the network.

Active users (*N*) are 50% of *n* connected nodes. *N* varies from 5 to 50 in simulations. *R* is the average user transaction rate for each phase. It is set to be 1 and 5 in simulations. γ is the unit packet transmission cost and $d_{SN\text{-}CN}$ denotes the average hop distance between SN and CN.

Pure P2P with IBC

Total transmission signaling cost by using pure P2P is:

$$C_{total}^{IBC} = C_{register}^{IBC} + C_{publish}^{IBC} + C_{search}^{IBC} + C_{retrieve}^{IBC}$$

Where, each transmission signaling phase is given by:

$$C_{register}^{IBC} = N^{*}R_{reg}\,(\gamma\,(2\,d_{SN\text{-}CN}))$$

$$C_{publish}^{IBC} = 0 \text{ (Nodes keep indexes, no publishing)}$$

$$C_{search}^{IBC} = N^{*}R_{sea}\,(\gamma\,(S_n^{cost}\,d_{SN\text{-}CN}))$$

$$C_{retrieve}^{IBC} = N^{*}R_{ret}\,(\gamma\,(7\,d_{SN\text{-}CN}))$$

SIP based with Http Digest

Total transmission signaling cost by using SIP based is:

$$C_{total}^{SIP} = C_{register}^{SIP} + C_{publish}^{SIP} + C_{search}^{SIP} + C_{retrieve}^{SIP}$$

Where, each transmission signaling phase is given by:

$$C_{register}^{SIP} = N^{*}R_{reg}\,(\gamma\,(\,4d_{SN\text{-}Proxy} + 4d_{Proxy\text{-}AAA})\,)$$

$$C_{publish}^{SIP} = N^{*}R_{pub}\,(\gamma\,(\,2d_{CN\text{-}Proxy} + 2d_{Proxy\text{-}Cat}\,)\,)$$

$$C_{search}^{SIP} = N^{*}R_{sea}\,(\gamma\,(\,2d_{SN\text{-}Proxy} + 2d_{Proxy\text{-}Cat})\,)$$

$$C_{retrieve}^{SIP} = N^{*}R_{ret}(\gamma\,(5d_{SN\text{-}Proxy} + 5d_{Proxy\text{-}Proxy} + 5d_{Proxy\text{-}CN})\,)$$

$d_{x\text{-}y}$ denotes hop distances from x to y where they are elements of SIP architecture

IMS with AKA

Total transmission signaling cost by using IMS is:

$$C_{total}^{IMS} = C_{register}^{IMS} + C_{publish}^{IMS} + C_{search}^{IMS} + C_{retrieve}^{IMS}$$

Where, each transmission signaling phase is given by:

$$C_{register}^{IMS} = N^{*}R_{reg}\,(\gamma\,(\,8d_{SN\text{-}Pcscf} + 4d_{Pcscf\text{-}Icscf} + 4d_{Icscf\text{-}HSS} + 4d_{Icscf\text{-}Scscf} + 4d_{Scscf\text{-}HSS})\,)$$

$$C_{publish}^{IMS} = N^{*}R_{pub}\,(\gamma\,(7d_{CN\text{-}Pcscf} + 7d_{Pcscf\text{-}Scscf} + 7d_{Scscf\text{-}AS}\,)\,)$$

$$C_{search}^{IMS} = N^{*}R_{sea}\,(\gamma\,(\,7d_{SN\text{-}Pcscf} + 7d_{Pcscf\text{-}Scscf} + 7d_{Scscf\text{-}AS}\,)\,)$$

$$C_{retrieve}^{IMS} = N^{*}R_{ret}\,(\gamma\,(7d_{SN\text{-}Pcscf1} + 7d_{Pcscf1\text{-}Scscf1} + 2d_{Scscf1\text{-}Icscf} + 5d_{Scscf1\text{-}Scscf2} + 2d_{Icscf\text{-}HSS} + 2d_{Icscf\text{-}Scscf2} + 7d_{Scscf2\text{-}Pcscf2} + 7d_{Pcscf2\text{-}CN}\,)\,)$$

$d_{x\text{-}y}$ denotes hop distances from x to y where they are elements of IMS architecture

Simulation and Comparison Evaluation

The trunked Pareto distribution is assumed for packet length with an average equal to 480 bytes (D. Tarchi, 2006). Data bit rate is 10 Mbps, and γ is equal to 3.84 x 10^{-4} sec.

In P2P, hop distance between SN and CN is averaged on 7, in SIP and in IMS, the distance from the user to the service network (i.e. $d_{S/CN\text{-}Proxy}$ in SIP, $d_{S/CN\text{-}P\text{-}CSCF}$ in IMS) is 3, counting on 2 routers between path on average; while the distance inside the service network (i.e. $d_{Proxy\text{-}Proxy}$ for SIP, and $d_{x\text{-}CSCF}$ $d_{y\text{-}CSCF}$ for IMS) is set to be 2 (A. Munir, 2008). Note that the value range is representative of real situation but of course another modeling, especially of P2P, would produce different values. Meanwhile, the result trends would be similar.

Fig. 6 and Fig. 7 indicate the transmission cost of communication that corresponds to active nodes and establishment in function of connected node number. There are 1 register, publishing, searching and retrieving per active node (R=1 for all phases) in Fig. 7, and 5 searching (R_{sea} = 5) in Fig. 8. Conformal to formula, the transmission cost grows with active users. SIP based has the lowest transmission cost. Pure P2P has the highest one, due to the flooding algorithm in searching phase (more sophisticated algorithm may be adopted). Moreover, it has more hop distance than others. The gap between IMS transmission cost and SIP one decreases with the number of searching per user. Thus, for a frequently used service, IMS and SIP do not have very different performance compared to pure P2P.

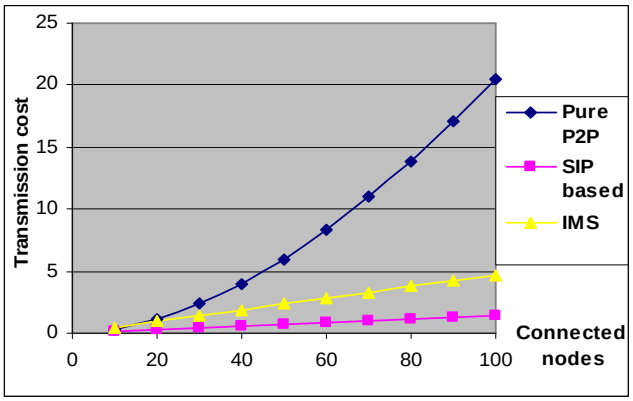

FIG. 6 TRANSMISSION COST WITH 1 REGISTRATION, PUBLISHING, SEARCHING RETRIEVING/USER

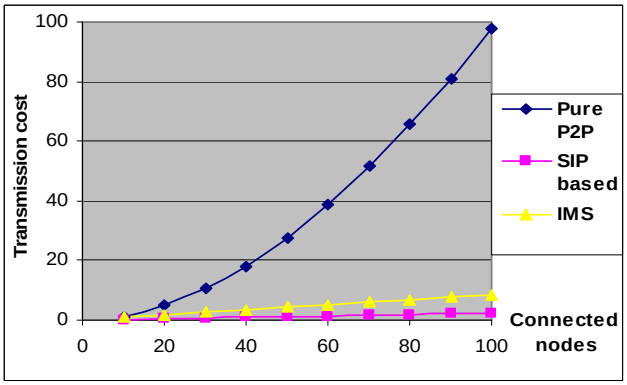

FIG. 7 TRANSMISSION COST WITH 1 REGISTRATION, PUBLISHING, RETRIEVING/USER AND 5 SEARCHING/USER

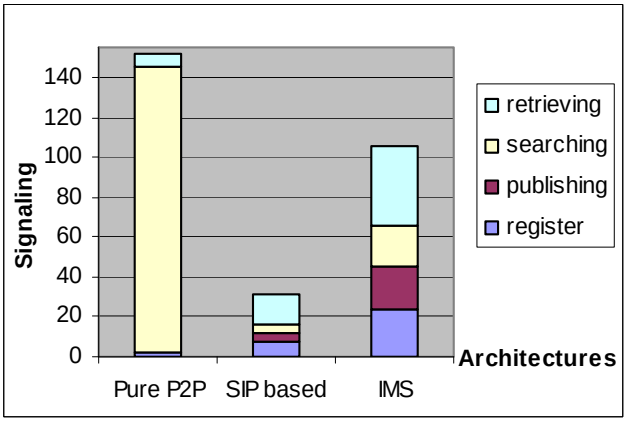

FIG. 8 SIGNALING IN NETWORK ARCHITECTURES FOR ONE SEARCHING

Signaling is detailed on Fig. 8. SIP has least signaling because it does not treat all SIP IMS standard signaling, (information is included in the SIP messages during publishing and searching) and it has less architecture components than IMS. Furthermore, IMS must open the session with SIP INVITE when it starts any connected phase (e.g., Publishing, Searching). The major cost in P2P is due to research. With a more sophisticated algorithm, a factor 2 of improvement could be obtained so that P2P could reach same level of performance as IMS. Although pure P2P has more signaling compared with SIP, each node does not handle too much signaling.

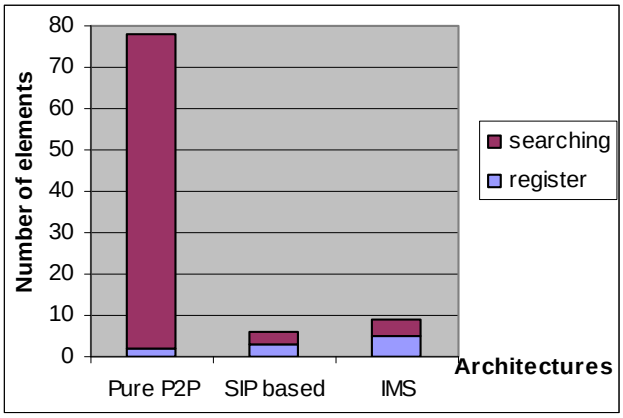

FIG. 9 PARTICIPATED NUMBER OF ELEMENTS IN ARCHITECTURES

When considering the number of entities which forward signaling in Fig. 9, it is seen that there are many nodes which work together in decentralized fashion for sharing resources. Signaling per node might not be very different with SIP based solution. On the other hand, the centralized catalogue server in SIP and in IMS handle many searching queries compare with pure P2P. Thus P2P is not so costly for a large number of service users in each node.

Deployment Assumption

Assumption for deployment is shown in Table1. IBC with pure P2P does not need to have pre-shared key, however, it also needs to have private key which correspond with its ID and system parameter. IBC can be well integrated in distributed environment while SIP based uses pre-shared to do HTTP digest with AAA server for session key generation and uses between its proxy. In addition, the proxy can be a firewall to protect the system from other intruders attacking the system (e.g., DoS attack). In the computation view, symmetric cryptography is used in SIP based that takes less computing time than asymmetric cryptography used in IBC too.

TABLE 1 : SECURITY ASSUMPTION FOR DEPLOYMENT

	Pure P2P	**SIP Based**	**IMS**
Setup	Private key correspond with ID and parameters	Pre-shared key between user and AAA	Pre-shared key between user and HSS
Trusted elements	PKG	Between proxy and AAA	CSCFs, AS and HSS
Security protocol	IBC Session key	HTTP Digest Session key	HTTP Digest IPSec

IMS uses centralized user profiles. All users must authenticate themselves through P/I/S-CSCFs components and establish IPSec tunnel between UEs and P-CSCF. Actually, our SIP based is quite similar to IMS architecture since they use a centralized catalogue and have a proxy to manage and protect a network. The main different between them are user profile location and CSCF components (e.g., I/S-CSCF, HSS).

All of the proposed network architectures provide authentication mechanisms to secure home services. These authentication mechanisms do not tie with a specific cryptograph algorithm. Network administrator freely chooses a suitable protocol (e.g., AES, 3DES, RSA, MD5 and SHA-1).

Conclusions

In this work, two network architectures were proposed for delivery home content to home users and then compared to IMS reference architecture, considering the scaling factor.

The focus was placed on authentication mechanisms which can be used for user identification to secure communities. In terms of security aspects and deployment, all considered architectures have some similarities since they required previously setup which can be done through home gateway configuration.

In terms of performance, architectures have been studied from their signaling. Photo sharing service is used to illustrate the function of presented architectures. It has been shown that SIP based has least signaling. Indeed, even if it presents a less complex architecture, it can still provide effective user authentication. In addition, the SIP solution can be improved by the use of SIP proxy (kind of firewall against intruders) but with a cost: more signaling and more complexity.

Considering the scaling factor, the analysis showed that for a successful service (frequently used), IMS performances are improved. For the P2P solution, signaling is too heavy and can be deployed only in

small communities. Nevertheless, the P2P solution can be highly improved by the use of an efficient research mechanism like, Distributed Hash Table. Experiments have been done with DHT P2P by implementing a SIP RELOAD architecture and this assumption has been confirmed.

REFERENCES

3GPP, "IP Multimedia Subsystem (IMS)," TS 23.228, Release 8, Version 8.7.0, Dec 08 Peer-to-Peer Lookup Protocol for Internet Applications, IEEE/ACM Transactions on Networking, Vol 11, Feb 2003

A. L. Barabasi and R. Albert, Emergence of Scaling in Random Networks, Science, pages 509-512, Oct 1999

A. Medina, A. Lakhina, I. Matta, and J.Byers, "BRITE: Boston university representative internet topology generator", Boston University, Apr 2001

A. Munir, W. Vincent and S. Wong, Interworking Architectures for IP Multimedia Subsystems, Computer science mobile networks and applications, Volume 12, Numbers 5-6, Springer Science, Apr 2008

A. Shamir, "Identity-based cryptosystems and signature schemes", Advances in Cryptology (Proceedings of Crypto '84), Lecture Notes in Computer Science, vol 196, Springer-Verllag, 1985

D. Tarchi, R. Fantacci, M. Bardazzi, Quality of service management in IEEE 802.16 wireless metropolitan area networks, In Proc of IEEE International conference on communication (ICC), Turkey, Jun 2006

I. F. Blake, G. Seroussi and N. P. Smart, Advances in Elliptic Curve Cryptography, Cambridge University Press, London mathematical Society Lecturer Note Series 317, 2005

J. Franks, P. Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen and L. Stewart, HTTP Authentication: Basic and Digest Access Authentication, RFC 2617, IETF Network Working Group, Jun 1999

M. Jovanovic, F. Annexstein, and K. Berman: Modeling peer-to-peer network topologies through "small-world" models and power laws, IX Telecommunications Forum TELFOR 2001, Belgrade, 2001

M. Jovanovic, Modeling large-scale peer-to-peer networks and a case study of Gnutella, MS. Thesis, University of Cincinnati, Cincinnati, Ohio, USA, 2001

P. Zimmermann, The Official PGP User's Guide. MIT Press, Cambridge, Massachusetts, 1995

V. Pathak and Iftode, Byzantine fault tolerant public key authentication in peer-to-peer systems, Computer Networks, Special Issue on Management in Peer-to-Peer Systems: Trust, Reputation and Security, 50(4): 579-596, Mar 2006

W. Werapun, A. Abou El Kalam, B. Paillassa, J. Fasson, "Solution Analysis for SIP Security Threats", International Conference on Multimedia Computing and Systems, ICMCS 2009, Apr 2009

Y. Zhang, S. Chen and G. Yang, SFTrust: A double trust metric based trust model in unstructured P2P system, 2009 IEEE International Symposium on Parallel & Distributed Processing, May 2009

Warodom Werapun received the Ph.D. degree from Institute National Polytechnique of Toulouse (INPT), France. During 2008-2010, he did a joint Feel@Home research project supported by European Celtic Project. He is currently an associate department head for administration at the department of computer engineering, Prince of Songkla University, Phuket Campus, Thailand; meanwhile, he is a deputy head of INFAR research group. His current areas of research are network architecture, P2P, SIP, routing protocol and security.

Julien Fasson has received a Ph.D. degree in Computer Systems and Telecommunications from the University of Toulouse in 2004. Since then, he has been an Assistant Professor at IRIT laboratory of Toulouse. His main interests are focused on the integration of satellite systems in terrestrial networks and the network architecture for service integration. In this context, he has worked on NGN architectures (IMS) and mobility issues in heterogeneous, including the use of MIH in a satellite/LTE context.

Beatrice Paillassa is Professor in computer networks at the ENSEEIHT engineer school. She earned a Ph.D in computer sciences and an "Habilitation a Diriger les Recherches" in computer networks from Toulouse university; in addition, member of the research team IRT "Network and Telecommunication Engineering" at the IRIT laboratory of Toulouse. Her research interests include communication protocol design and analysis, modeling, and architecture specification. She currently works on convergence architecture, satellite networks and wireless protocols.