Ecole Doctorale EDITE

Thèse présentée pour l'obtention du diplôme de Docteur de Télécom & Management SudParis

Doctorat conjoint Télécom & Management SudParis et Université Pierre et Marie Curie

Spécialité : informatique et réseaux

Par

Songbo SONG

Advanced Personalization of IPTV Services

Soutenue le 06/01/2012 devant le jury composé de :

Pascal LORENZ	Rapporteur	University of Haute Alsace
Ken CHEN	Rapporteur	University of Paris 13
Guy PUJOLLE	Examinateur	University of Pierre et Marie Curie
Gilles BOURDON	Examinateur	Orange France
Stéphane BETGE-BREZETZ	Examinateur	Alcatel Lucent Bell Labs France
Laurent RUCKENBUSCH	Examinateur	France Telecom - Orange Labs
Hassnaa MOUSTAFA	Co-Directeur de thèse	France Telecom - Orange Labs
Hossam AFIFI	Directeur de thèse	Institut Telecom SudParis

Thèse n° 2012TELE0001

Thèse n° 2012TELE0001

Ecole Doctorale EDITE

Thèse présentée pour l'obtention du diplôme de
Docteur de Télécom & Management SudParis

Doctorat conjoint Télécom & Management SudParis et Université Pierre et Marie Curie

Spécialité : informatique et réseaux

Par
Songbo SONG

Individualisation Avancée des Service IPTV

Soutenue le 06/01/2012 devant le jury composé de :

Pascal LORENZ	Rapporteur	University of Haute Alsace
Ken CHEN	Rapporteur	University of Paris 13
Guy PUJOLLE	Examinateur	University of Pierre et Marie Curie
Gilles BOURDON	Examinateur	Orange France
Stéphane BETGE-BREZETZ	Examinateur	Alcatel Lucent Bell Labs France
Laurent RUCKENBUSCH	Examinateur	France Telecom - Orange Labs
Hassnaa MOUSTAFA	Co-Directeur de thèse	France Telecom - Orange Labs
Hossam AFIFI	Directeur de thèse	Institut Telecom SudParis

Thèse n° 2012TELE0001

Thèse n° 2012TELE0001

Abstract

Internet Protocol TV (IPTV) delivers television content to users over IP-based network. Different from the traditional TV services, IPTV platforms provide users with large amount of multimedia contents with interactive and personalized services, including the targeted advertisement, on-demand content, personal video recorder, and so on. IPTV is promising since it allows to satisfy users experience and presents advanced entertainment services. On the other hand, the Next Generation Network (NGN) approach in allowing services convergence (through for instance coupling IPTV with the IP Multimedia Subsystem (IMS) architecture or NGN Non-IMS architecture) enhances users' experience and allows for more services personalization. Although the rapid advancement in interactive TV technology (including IPTV and NGN technologies), services personalization is still in its infancy, lacking the real distinguish of each user in a unique manner, the consideration of the context of the user (who is this user, what is his preferences, his regional area, location, ..) and his environment (characteristics of the users' devices 'screen types, size, supported resolution, …' and networks available network types to be used by the user, available bandwidth, ..') as well as the context of the service itself (content type and description, available format 'HD/SD', available language, ..) in order to provide the adequate personalized content for each user. This advanced IPTV services allows services providers to promote new services and open new business opportunities and allows network operators to make better utilization of network resources through adapting the delivered content according to the available bandwidth and to better meet the QoE (Quality of Experience) of clients.

This thesis focuses on enhanced personalization for IPTV services following a user-centric context-aware approach through providing solutions for: i) Users' identification during IPTV service access through a unique and fine-grained manner (different from the identification of the subscription which is the usual current case) based on employing a personal identifier for each user which is a part of the user context information. ii) Context-Aware IPTV service through proposing a context-aware system on top of the IPTV architecture for gathering in a dynamic and real-time manner the different context information related to the user, devices, network and service. The context information is gathered throughout the whole IPTV delivery chain considering the user domain, network provider domain, and service/content provider domain. The proposed context-aware system allows monitoring user's environment (devices and networks status), interpreting user's requirements and making the user's interaction with

the TV system dynamic and transparent. iii) Personalized recommendation and selection of IPTV content based on the different context information gathered and the personalization decision taken by the context-aware system (different from the current recommendation approach mainly based on matching content to users' preferences) which in turn highly improves the users' Quality of Experience (QoE) and enriching the offers of IPTV services.

The proposed solutions in this thesis are implemented in a real IPTV platform as a proof of concept and their performance is evaluated through several metrics defined within the thesis work.

Acknowledgements

This dissertation marks the end of my journey as a student at INT. My accomplishment over the past three years is indebted to many people. Especially, I want to thank my supervisor, Prof. Hossam Afifi, for his patience with all my questions and stupendous effort on guiding my research and reviewing my papers. Thank you, Prof. Hossam Afifi, I am very grateful.

I am also deeply indebted to co-supervisor Dr.Hassnaa Moustafa. She is a great advisor and a fantastic friend, and in my mind, she is very nice and rigorous. It was with her that I first learned how to do research and how to write scientific papers. She gives me extremely valuable remarks regarding the style and scientific contributions of this thesis. Her favorite quote “Do not be nervous, we will find the solution" encouraged me a lot when I do research.

I owed much to my committee members. Thank you, Pascal LORENZ, Ken CHEN, Guy PUJOLLE, Gilles BOURDON, Stéphane BETGE-BREZETZ and Laurent RUCKENBUSCH for accepting to review my dissertation and to be member of my Phd defense jury.

I also extend my thanks to all my colleagues and group members in Orange R&D lab. In particular I appreciate Laurent RUCKENBUSCH for giving me the opportunity to work in Orange R&D lab and his availability for support and help. I also want to thank Aurélien Violet, Didier Gorges and Jean-Baptiste Hennequin, from whom I have picked up much knowledge on IPTV.

Coming to study in France was a turning point in my life. I would like to thank my parents for the tremendous sacrifices they have made. They have done everything possible to ensure that I had a good education. For this and much more, I am forever in their debt. Thank you, Mom and Dad.

Contents

List of Figure

Résumé

Individualisation Avancée des Service IPTV

1 Introduction

Le monde de la TV est en cours de transformation de la télévision analogique à la télévision numérique, qui est capable de diffuser du contenu de haute qualité, offrir aux consommateurs davantage de choix, et rendre l'expérience de visualisation plus interactive. IPTV (Internet Protocol TV) présente une révolution dans la télévision numérique dans lequel les services de télévision numérique sont fournis aux utilisateurs en utilisant le protocole Internet (IP) au dessus d’une connexion haut débit. Les progrès de la technologie IPTV permettra donc un nouveau modèle de fourniture de services. Les fonctions offertes aux utilisateurs leur permettent de plus en plus d’autonomie et de plus en plus de choix. Il en est notamment ainsi de services de type ‘nTS’ (pour ‘network Time Shifting’ en anglais) qui permettent à un utilisateur de visionner un programme de télévision en décalage par rapport à sa programmation de diffusion, ou encore des services de type ‘nPVR’ (pour ‘network Personal Video Recorder’ en anglais) qui permettent d’enregistrer au niveau du réseau un contenu numérique pour un utilisateur. D'autre part, l'architecture IMS proposée dans NGN fournit une architecture commune pour les services IPTV.

Malgré les progrès rapides de la technologie de télévision interactive (comprenant notamment les technologies IPTV et NGN), la personnalisation de services IPTV en est encore à ses débuts. De nos jours, la personnalisation des services IPTV se limite principalement à la recommandation de contenus et à la publicité ciblée. Ces services ne sont donc pas complètement centrés sur l’utilisateur, alors que choisir manuellement les canaux de diffusion et les publicités désirées peut représenter une gêne pour l’utilisateur. L’adaptation des contenus numériques en fonction de la capacité des réseaux et des dispositifs utilisés n’est pas encore prise en compte dans les implémentations actuelles. Avec le développement des technologies numériques, les utilisateurs sont amenés à regarder la télévision non seulement sur des postes de télévision, mais également sur des smart phones, des tablettes digitales, ou encore des PCs.

En conséquence, personnaliser les contenus IPTV en fonction de l'appareil utilisé pour regarder la télévision, en fonction des capacités du réseau et du contexte de l'utilisateur représente un défi important.

Trois étapes sont nécessaires pour réaliser la personnalisation de services IPTV, comme l'illustre la figure 1:

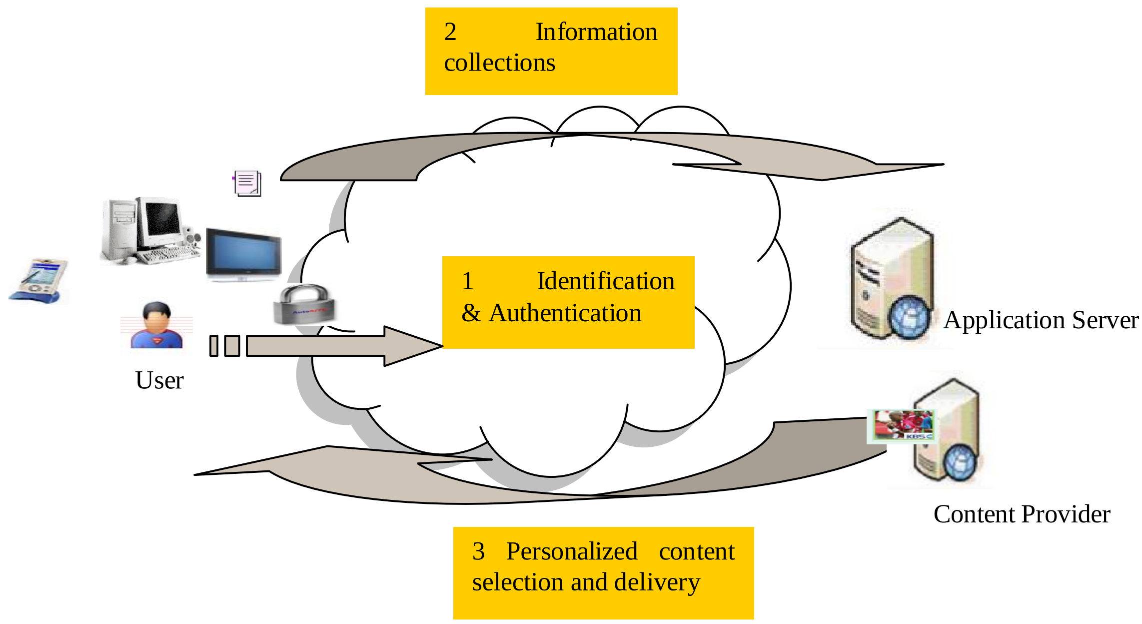


Figure 1 La personnalisation de services IPTV

- Pour offrir un service personnalisé, le système a besoin d'être conscient des identités des utilisateurs actuels en face de la télévision. Différents techniques d'identification et d'authentification peuvent être appliquées au système IPTV, par exemple : l'identification biométrique, identification par radiofréquence (RFID), ou simple avec l'ID utilisateur et mot de passe.
- Après l'identification de l'utilisateur, le système sélectionne les contenus personnalisés pour l'utilisateur. Les sélections des contenus personnalisées doivent non seulement tenir compte des préférences de l'utilisateur, mais aussi besoin de considérer les contextes. Par exemple, si un utilisateur choisit de regarder la télévision dans un dispositif qui ne supporte pas la HD, le système de recommandation ne devrait pas

proposer des contenus HD pour lui. Aussi, l'adaptation de contenu doit être assurée de manière dynamique avec les changements des contextes différents. Pour la personnalisation des services IPTV, un système sensible au contexte sur le dessus de l'architecture IPTV rassemble dynamiquement les informations de contexte différent lié à l'utilisateur, dispositifs, réseaux et services.

- La prise en compte du contexte pourrait permettre une personnalisation des services IPTV adaptée à chaque utilisateur (d'une manière différenciée), and adaptée à l'environnement de l'utilisateur (dispositif et réseau). Selon les préférences utilisateur et les contextes, des contenus personnalisés sont sélectionnés par le système. Le Guide du Programme électronique personnalisé est utilisé pour informer l'utilisateur sur l'ensemble des contenus qui sont appropriés pour lui. Lors de la livraison des contenus, le format du contenu peut être automatiquement adapté à la capacité du réseau et le dispositif utilisé. En outre, le service de notification pourrait être utilisé pour avertir l'utilisateur qu'un meilleur contenu est disponible (plus adapté à l'utilisateur selon ses préférences ou des informations de contexte).

2 La personnalisation de services IPTV à travers la sensibilité au contexte

Des systèmes sensibles au contexte jouent un rôle très important dans les systèmes informatiques modernes. Hull et coll. [Hull 97] a défini la sensibilité au contexte comme la capacité du système à détecter et à interpréter les informations dans l'environnement et adapter les services à ces informations. Donc une application IPTV sensible au contexte est une application qui s'exécute dans un environnement IPTV et qui adopte l'utilisation des contextes pour fournir des services.

2.1 Les types des informations de contexte pour IPTV

Pour la personnalisation des services IPTV, les types des informations de contexte doivent couvrir toute la chaîne IPTV, y compris le domaine de l'utilisateur, le domaine du fournisseur de réseau, le domaine du fournisseur de service et le domaine du fournisseur de contenu. Donc il y a quatre types d'informations de contexte pour IPTV sensible au contexte :

- Informations de contexte d'utilisateur : comprennent des informations sur l'utilisateur qui pourraient être des informations statiques, des informations dynamiques et des informations inférées. Des informations statiques représentent les informations personnelles de l'utilisateur qui ne change pas pendant une longue période et stockées dans la base de données, y compris le profil de l'utilisateur, les préférences statiques de l'utilisateur. Ces informations sont explicitement données par l'utilisateur lors de l'abonnement au service. Les informations dynamiques changent fréquemment, et y comprennent la position de l'utilisateur, l'agenda et l'émotion de l'utilisateur, etc. Les informations dynamiques sont capturées par des capteurs ou par d'autres services. Les informations inférées sont les contextes de plus haut niveau qui sont acquises par l'analyse des autres informations.
- Informations de contextes de dispositif : présentent les informations sur les dispositifs qui pourraient être la taille des écrans, la capacité de connectivité (GPRS, 3G, Wi-Fi), sa proximité avec les utilisateurs ainsi que l'état des dispositifs (éteint ou non).
- Information de contexte de réseaux : présentent les informations sur les réseaux qui pourraient être le type de réseau d'accès, bande passante disponible et l'état de charge de réseau (gigue, taux de perte de paquets, retard, etc),
- Information de contexte de service : présentent les informations concernant la description du contenu et du media. La description du contenu fournit des informations générales sur le contenu, comme le titre, mot clé, réalisateur, acteur, genre, durée, et la langue. La description du media représente le format codec de contenu (par exemple format MPEG2, MPEG4, AVC ou AVS), résolution (haute définition ou standard définition), etc.

Une modélisation graphique pour modéliser ces informations de contexte est proposée dans la thèse. Cette modélisation définit un certain nombre de classes et les attributs qui présentent les informations de contexte utilisés pour les services d'IPTV qui couvrent toutes les chaînes de service IPTV: utilisateur, dispositif, réseau et services.

2.2 Architecture générale d'un système sensible au contexte

Une architecture générale d'un système sensible au contexte est proposée dans la thèse qui contient quatre parties comme l'illustre la figure 2.

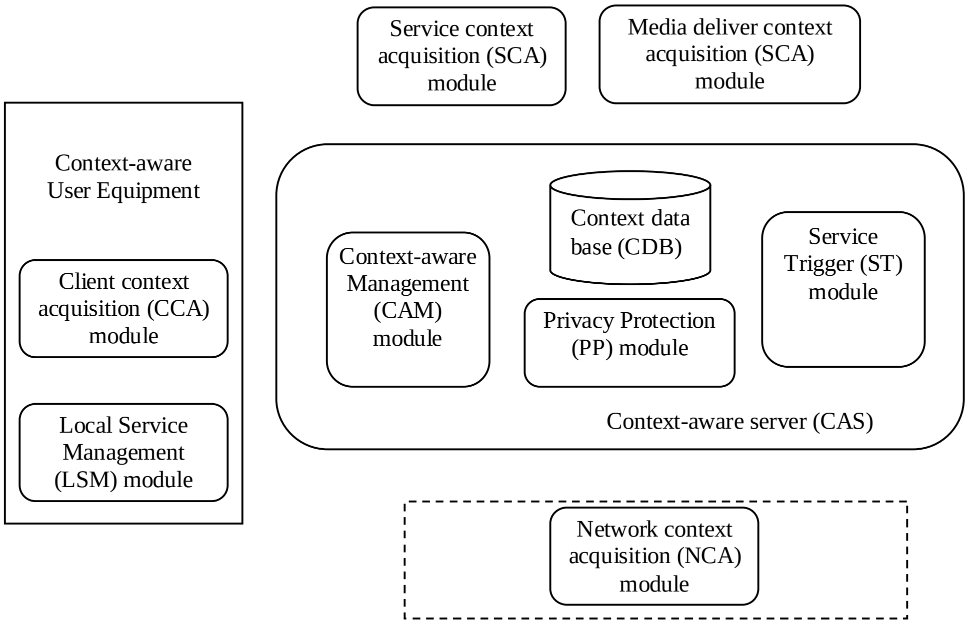


Figure 2 Architecture générale d'un système sensible au contexte

1) Dans le cœur de réseau de l'opérateur, un server centrale (CAS, Context-aware Server) est situé de façon centrale) est utilisé pour contrôler les contextes et permettre des services personnalisés pour l'utilisateur. Le CAS comprend quatre modules:

- un module de gestion prenant en compte le contexte (CAM, Context-Aware Management Module). Ce module rassemble les informations de contexte obtenues de l'utilisateur, du dispositif, du serveur applicatif et du réseau, et dérive des informations de contexte de plus haut niveau par inférence de contexte.
- un module de base de données de contexte (CDB, Context DataBase). Ce module stocke les informations de contexte rassemblées et obtenues par inférence, et fournit une interface de requête à un module de déclenchement de service (ST).
- un module de déclenchement de service (ST Service Trigger). Ce module offre deux fonctions: personnalisation de services établis, en fonction des diverses informations

de contexte, et découverte et configuration de services personnalisés pour les utilisateurs en fonction des différents contextes. Le module ST communique dynamiquement avec le module CDB pour observer les informations de contexte. Avant de déclencher les services, il communique avec le module de protection de la vie privée (PP) pour vérifier si les services peuvent utiliser les informations de contexte ou s'il existe des contraintes de vie privée.

- un module de protection de la vie privée (PP Privacy Protection). Ce module effectue des contrôles pour déterminer quelles données peuvent être utilisées en vérifiant si les services prêts à être activés ont l'autorisation d'accéder aux informations de contexte requises ou à un sous ensemble, en fonction de différent de niveaux de protection de la vie privée.

2) Dans l'équipement utilisateur il y a deux modules : Le module CCA (Client Context Acquisition) découvre les sources de contexte dans la sphère locale et collecte l'information de contexte brute (information de contexte d'utilisateur et de contexte de dispositif) puis l'envoie au module CAM situé dans le serveur CAS; Le module LSM (Local Service Management) contrôle et gère l'exécution des services locaux à l'aide du suivi du module CCA et de la comparaison dynamique du contexte avec ses règles stockées, de façon à activer un service correspondant de façon personnalisée.

3) Les modules de domaines de services situés au niveau des serveurs applicatifs comprennent un module d'acquisition de contexte de service (SCA Service Context Acquisition) qui collecte de l'information de contexte de service et la transmet au module CAM, et un module d'acquisition de contexte de fourniture de media (MDCA Media Delivery Context Acquisition) qui observe la fourniture de contenu et acquiert dynamiquement de l'information de contexte réseau durant la fourniture de service et l'envoie au module CAM.

(4) Dans le domaine réseau, un module d'acquisition de contexte réseau (NCA Network Context Acquisition) collecte de l'information de bande passante en consultant le sous-système de contrôle de ressource et d'admission (RACS, Resource and Admission Control Sub-System) avant l'établissement de chaque session de service et envoie l'information acquise au module CAM.

2.3 Système de personnalisation de service IPTV basée sur IPTV/IMS architecture

La figure 3 représente une extension d'une architecture IPTV/IMS par intégration d'un système sensible au contexte pour personnaliser des services IPTV.

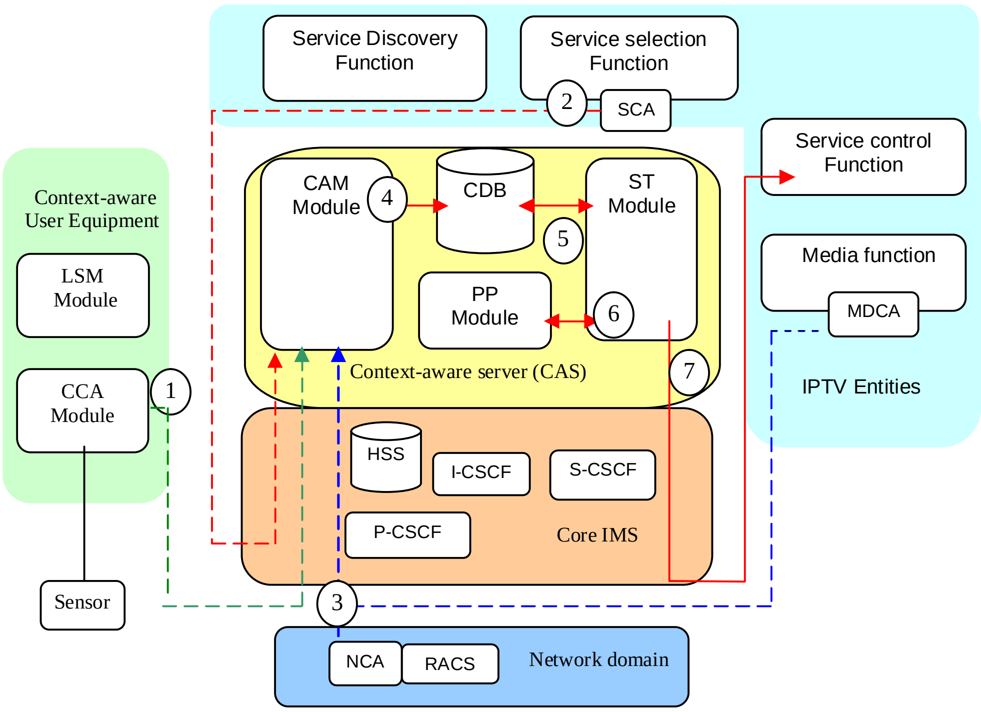


Figure 3 Système de personnalisation de services IPTV basé sur IPTV/IMS architecture

Cette architecture utilise le HSS pour stocker les statiques informations de l'utilisateur, qui contient informations personnelles de l'utilisateur (âge, sexe ...), les services auxquels il est abonné, ainsi que ses préférences

- Le module SCA est intégré dans l'IPTV Service Selection fonctionnels (SSF) module et acquiert les informations de contexte de service utilisant un guide de services électronique (ESG Electronic Service Guide) reçu par le module SSF de la part d'un fournisseur de contenus, et qui inclut une description du contenu et du média.
- Le module d'acquisition de contexte de fourniture de média MDCA est intégré dans la fonction média (MF) pour acquérir dynamiquement des informations sur le réseau. Le module MF emploie le protocole RTCP (Real Time Transport Control Protocol) pour contrôler la fourniture de contenu en rassemblant dynamiquement des statistiques

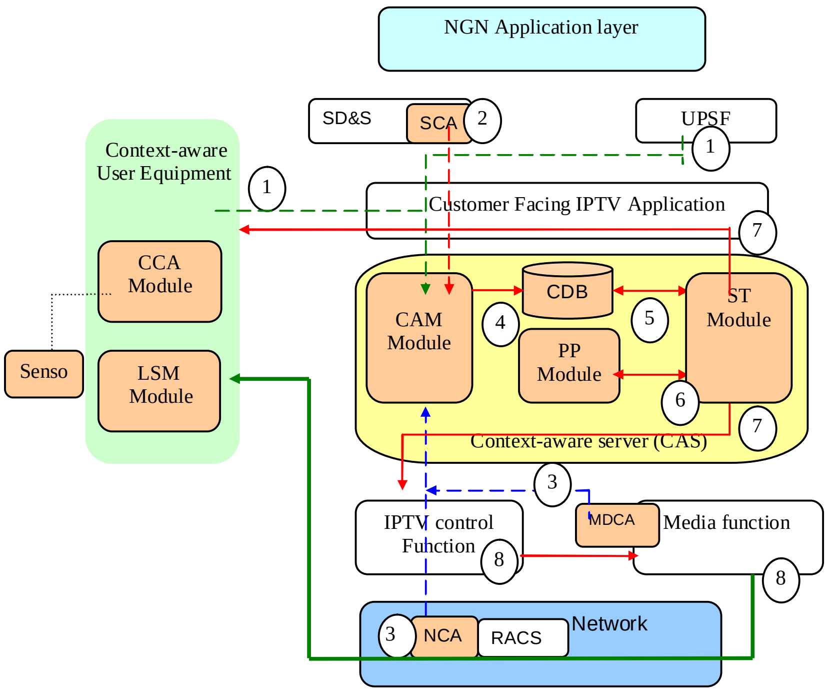
d’informations réseau pour une session média, par exemple des informations concernant les pertes de paquets, la gigue, ou le temps aller-retour (round-trip delay), qui reflétant le contexte réseau.

- D'autre part, le module d’acquisition de contexte réseau NCA est intégré au sein d’un sous-système de contrôle de ressources et d’admission (RACS) afin de collecter les informations de contexte initiales (telles que la bande passante).
- Le module d’acquisition de contexte client CCA et le module de gestion de services locaux LSM est mise en place au sein de l’équipement utilisateur UE (smart phone, etc.).

Après chaque acquisition d’informations de contexte (liées par exemple à l’utilisateur, au dispositif, au réseau et aux services offerts) (étapes 1-3), le module CAM dans le serveur CAS stocke les informations collectées dans la base de données de contexte CDB (étape 4). Le module de déclenchement de service ST peut communiquer de façon continue avec le module CDB pour suivre l’évolution information de contexte et découvrir un besoin de personnaliser des services établis ou de configurer de nouveaux services (étape 5). Et puis, le module ST obtient des informations de contexte stockées dans la base de données de contexte CDB et les utiliser lors du déclenchement d’un service correspondant. Avant de déclencher le service, le module ST communique avec le module PP (privacy protection) pour vérifier si le service correspondant peut complètement utiliser l’information de contexte existante (étape 6). S’il n’existe pas de contrainte de protection de la vie privée, le module ST envoie à la fonction de commande de service (SCF) d'un message pour déclencher le service, en encapsulant les informations de contexte nécessaires à ce message (étape 7).

2.2 Système de personnalisation de service IPTV basée sur IPTV/Non-IMS architecture

Dans le système IPTV sensible au contexte basé sur IMS, le cœur IMS est responsable du contrôle de la signalisation et du transfert de l’information de contexte vers le serveur. Le cœur IMS facilite le déploiement. Cependant la solution basée sur l’IMS s’appuie sur le protocole SIP, ce qui limite son application en excluant les applications non-SIP et impose le déploiement d’une architecture IMS. En effet, avec le développement des services IPTV NGN, la coopération entre les opérateurs de réseaux et les fournisseurs de services devient cruciale. L'architecture générale basée sur la plateforme IPTV est très importante. Ne pas se lier à une architecture IMS qui est basée sur le protocole SIP permet d'accroître les possibilités de coexistence de différents systèmes IPTV appartenant à différents opérateurs de réseaux et fournisseurs de services. Cela améliore la compatibilité des services IPTV.



1. User and device context information and transmission
2. Service context information and transmission
3. Network context information and transmission
4. Context information storage in the CDB.
5. ST communication with the CDB for monitoring context information and services discovery.
6. ST communicates with the PP for privacy constraints verification.
7. ST requests to trigger the personalized services.
8. Adapted content to the UE

Figure 4 Système de personnalisation de services IPTV sans IMS

La figure 4 représente une extension d'une architecture IPTV/Non-IMS par intégration d'un système sensible au contexte pour personnaliser des services IPTV. Dans cette architecture, le protocole HTTP est utilisé comme protocole de signalisation pour transmettre l'information de contexte et pour contrôler les services. Le module serveur de profil utilisateur (UPSF) est utilisé pour stocker les statiques informations de contexte de utilisateur, telles que l'âge ou le sexe de l'utilisateur, les services auxquels il est abonné, ainsi que ses préférences. Le module SCA (Service Context Acquisition) est intégré dans le module Découverte et sélection de services (SD&S) et acquiert des informations de contexte de service utilisant un guide de services électronique (ESG Electronic Service Guide) reçu par le module SD&S de la part d'un fournisseur de contenus, et qui inclut une description du contenu et du média. Le module d’acquisition de contexte de fourniture de média MDCA et le module d’acquisition de contexte réseau NCA sont intégrés dans le Media Function (MF) et d’un sous-système de contrôle de ressources et d’admission (RACS).

Cette solution est mise en œuvre sur une plate-forme IPTV. Une évaluation de la performance est faite. Des résultats intéressants sont obtenus en termes des délais de sélection de contenu personnalisé et d'initiation de service ainsi que le temps de navigation d’EPG. Les résultats prouvent la réussite du système proposé.

3 Nouvelle identification et authentification pour les services IPTV

Pour personnaliser des services IPTV, le système a besoin de connaître l'utilisateur qui est en train de regarder la télévision. Identifier chaque utilisateur permet au système IPTV de savoir « qui est en train de regarder la télévision » et de personnaliser les contenus en conséquence. En effet, l'identité d’utilisateur est une partie du contexte de l'utilisateur.

L'identification des utilisateurs et la solution d'authentification doivent être appliquées à l'IPTV système afin d'identifier chaque utilisateur et personnaliser son accès. Authentification et la protection de l’information observent beaucoup d'attention dans les réseaux NGN, où l'authentification des utilisateurs à l'IMS a lieu via le protocole AKA (Authentication and Key Agreement). L'GBA (Generic Bootstrapping Architecture) est utilisé pour authentifier les utilisateurs avant d'accéder à des services multimédias via HTTP. Cependant l'attachement de l'authentification de l’utilisateur à son équipement limite la personnalisation des services et ne permet pas d'identification unique pour chaque utilisateur si plusieurs utilisateurs partagent le même équipement. Pour résoudre ce problème, une nouvelle identification et authentification solution utilisant la technologie RFID et de l'IBC (Identity Based cryptography) est proposé dans cette thèse.

La solution d'authentification SA-IBC est basé sur le GBA architecture. qui se compose de quatre entités: l’UE (User Equipment), le NAF (Network Application Function), le BSF (Bootstrapping Server Function) et le HSS (Home Subscriber Server). Le lecteur RFID est intégré dans l'UE, où chaque utilisateur a besoin du RFID pour s'identifier au système.

L'identité de l'utilisateur (UserID) et mot de passe sont stockés sur le étiquette RFID. Lorsque l'étiquette est lue par un lecteur RFID, l'identité de l'utilisateur et mot de passe sont transférés de l'étiquette RFID au lecteur RFID et puis au dispositif.

L'IBC mécanisme est utilisé pour générer les clés privées de l'UE au lieu d'utiliser des mécanismes AKA pendant la GBA authentification pour personnaliser les services. IBC est un cryptosystème dans lequel la clé publique est générée en utilisant l'identité de l'utilisateur. Il a une autorité de confiance centrale nommée PKG (Private Key Generator) qui utilise un secret maître pour générer des clés privées des utilisateurs. Chaque utilisateur doit s'authentifier à l'PKG et obtenir la clé privée pour déchiffrer les messages reçus, qui sont cryptés avec la clé publique de l'utilisateur. Dans la solution proposée, le PKG est intégré dans le Home Subscriber Server (HSS), sans modifier la fonction traditionnelle d'HSS.

La performance est un facteur important à considérer lors de la conception des protocoles d'authentification. l'Open BCMP (Baskett Chandy Muntz Palacios) modèle est employée pour évaluer la performance de la solution d'authentification proposée. Afin d'améliorer les performances de la solution d'authentification, un algorithme de clustering est également proposé qui distribue les serveurs d'authentification au sein de l'architecture SA-IBC selon le taux de service du système. Le modèle BCMP pour SA-IBC est implémenté sous Matlab et la performance est évaluée par la mesure de l'utilisation des services et le délai d'authentification. Il est observé que l'augmentation du nombre de clients a un impact sur l'utilisation des serveurs et le délai d'authentification. Par ailleurs, on observe que le BSF représente un goulot d'étranglement dans le processus d'authentification de service, où l'algorithme de clustering proposée est prouvé pour améliorer les performances du système.

4 Système de recommandation de contenus sensible au contexte

On assiste aujourd'hui à une explosion de la télévision numérique sur Internet (ou IPTV pour Internet Protocol TeleVision) et aux services associés, comme par exemple les services d'enregistrement de programmes numériques personnalisés (nTS network Time Shifting ou nPVR pour network PersonalVideo Recorder).

Compte-tenu de la multitude de programmes audiovisuels numériques diffusés chaque jour sur Internet, il est difficile pour un utilisateur d'identifier rapidement un programme adapté à ses goûts et à son environnement. Pour faciliter le choix de l'utilisateur, les opérateurs envisagent la mise en place de services de recommandation de programmes, destinés à proposer à l'utilisateur une liste de programmes personnalisés.

Un système de recommandation de contenus est proposé dans cette thèse, qui génère une liste de recommandation en prenant en compte les préférences de l'utilisateur (définies explicitement par l'utilisateur lors de la souscription au service de recommandation ou extraites à partir d'un historique des programmes précédemment visualisés par l'utilisateur), ainsi que l'impact du contexte de visualisation dans lequel se trouve l'utilisateur sur les contenus qu'il visualise (ex. moment de la journée, localisation de l'utilisateur, etc.). Cet impact reflète la préférence de l'utilisateur pour un type de contenus en fonction du contexte dans lequel il se trouve.

La figure 5 illustre l'architecture du système proposé, qui contient quatre éléments: un module de distribution de contexte, le module de filtrage de contenu, le module de contenu ordonnant et le module de recommandation.

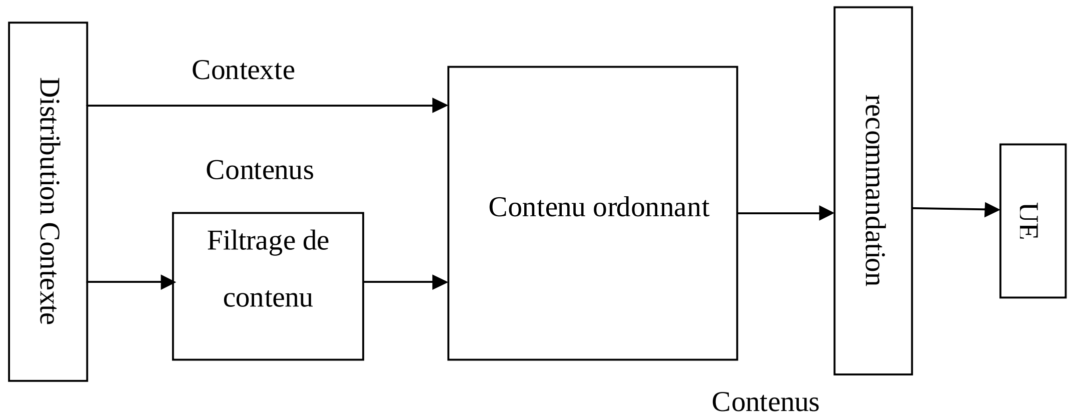


Figure 5 Système de recommandation de contenus sensible au contexte

- Le module de distribution de Contexte : il collecte des informations concernant un contexte de l'utilisateur à partir du serveur sensibles au contexte et les envoie au module de filtrage de contenu.
- Le module de filtrage de contenu : il s'agit d'établir un filtrage des contenus audiovisuels numériques proposés à l'utilisateur en prenant en compte des informations statiques liées à l'utilisateur ou à son environnement qui sont

susceptibles de conditionner l’accès aux contenus par l’utilisateur, comme son âge, la capacité de ses équipements, la capacité du réseau, la souscription ou non à des chaînes payantes, etc. Par exemple, si les capacités des équipements de l’utilisateur ne supportent pas la télévision Haute Définition, tous les contenus comprenant cette caractéristique sont éliminés. De façon similaire, tous les contenus qui ne sont pas autorisés pour l’utilisateur, par exemple de l’âge de l’utilisateur ou d’un accès restreint de l’utilisateur à certaines chaînes (ex. chaîne payante), sont supprimés. A la fin de filtrage, ce module envoie les contenues restes au module de contenu ordonnant.

- Le module de contenu ordonnant : il réalise un classement des contenus par ordre de préférence « implicites » de l’utilisateur. Par « préférences implicites », on entend ici des préférences qui ne sont pas explicitement définies par l’utilisateur (notamment lors de la souscription au service), mais estimées par le module de contenu ordonnant à partir de l’historique de visualisation de l’utilisateur. Les préférences « implicites » de l’utilisateur aussi reflet les relations entre les préférences de utilisateur et les contextes (i.e. de la situation) dans lequel l’utilisateur se trouve. Par exemple :
    - l’utilisateur regarde rarement la télévision numérique à 4 heures ; toutefois quand il regarde la télévision à 4 heures, il regarde un journal d’informations ; et
    - l’utilisateur regarde fréquemment la télévision dans le salon ; et la plupart du temps, quand il regarde la télévision dans le salon, il regarde des films.
- Le module de recommandation : Il génère le Guide du Programme personnalisé électronique (EPG) et l'envoie à l'utilisateur.

Ce système est mis en œuvre et il est évalué sur deux aspects: le retard de la recommandation qui mesure le temps passé pour la recommandation et la précision de la recommandation de contenu qui indique si le système pourrait recommander le bon contenu à l'utilisateur et reflète la satisfaction des utilisateurs pour une recommandation donnée.

5 Conclusion

Le domaine de la personnalisation des services IPTV est un vaste. Cette thèse a enquêté sur plusieurs problèmes qui sont importants pour offrir des services IPTV personnalisation et a présenté plusieurs contributions à la recherche de ces problèmes. Cette thèse présente des solutions visant à améliorer la personnalisation de services IPTV à partir de trois aspects:

1) Nouvelle architecture IPTV intégrée et comportant un système de sensibilité au contexte pour le service de personnalisation.

2) Nouvelle identification et authentification pour services IPTV

3) Nouveau service de recommandation de contenu en fonction des préférences de l'utilisateur et aussi des informations contextes.

Les perspectives pour les travaux futurs sont :

Développement d'un modèle d'OpenTV : le système sensible au contexte proposé peut être intégré dans les autres systèmes de télévision tels que la télévision sur Internet ou la télévision sur mobile.

Plus de moyens de personnalisation du service peut être considérés : par exemple, (1) le serveur de médias pourrait adapter le format du contenu dynamiquement selon les informations de contexte de réseau ; (2) le contenu personnel d'un utilisateur peuvent être transférées à partir d'un terminal à un autre terminal sans interrompre le service en fonction du changement de la position de l'utilisateur ; (3) le IPTV système sensible au contexte pourrait aussi coopérer avec d'autres services (par exemple le service de présence ou les applications des réseaux sociaux) pour fournir des services personnalisés avancés.

Introduction

TV is being transformed from the analog TV to the digital TV, which is able to stream content to high-quality, offer consumers more choice and make the viewing experience more interactive. IPTV (Internet Protocol TV) presents a revolution in digital TV in which digital television services are delivered to users using Internet Protocol (IP) over a broadband connection.

The advances in IPTV technology enable a new model for service provisioning, moving from traditional broadcaster-centric TV services to a new user-centric TV model which allows users not only to access new services and functionalities from their providers, but also to become active parts in the content personalization through contributing in building their dynamic profiles. With the consolidation of services, such as network Time Shifting (nTS) and network Personal Video Recorder (nPVR), users are allowed to record their own content and could also make them available to other users. On the other hand, the Next Generation Network (NGN) approach in coupling IPTV with the IP Multimedia Subsystem (IMS) architecture allows for services' convergence through using the IMS common architecture in providing a platform for interactive TV services.

In this context, IPTV has become increasingly focused on personalization and individualization, which allows content/service providers and networks operators to create new business opportunities and to promote smart and targeting services, while enhancing users' interaction with the IPTV system and the Quality of Experience (QoE) which in turn increases users' satisfaction and services acceptability.

The existing IPTV system shows some limitations at the level of services personalization. Although the rapid advancement in IPTV technologies, choosing the desired channel and the corresponding user profile in a manual mean could disturb the viewer. Users need to take a long time to find a content in which they are interested. Providing personalized service through the distinguishing of each user in a unique manner and the consideration of the context of the user and his environment (devices and network) still presents a challenge.

Contribution

This thesis aims to investigate the challenges and solutions allowing the enriched personalization of IPTV service, which seeks to cope with the current IPTV system limitations through distinguishing each user in two main manners: i) a context-aware manner considering the user context as well as the network, the terminals, and services contexts; and ii) an individual manner applying advanced and appropriate identification techniques, which are user-friendly and do not demand continuous intervention of the users. The main contributions contains:

1) Context-Aware IPTV architecture for enriched personalization

To provide new IPTV service and improve the user experience, this thesis proposes a context-aware IPTV architecture that extends the existing IPTV/IMS and IPTV/non-IMS architectures through integrating a context-awareness system. In this architecture, rich context information related to the user, device, network and service are considered and organized through a new IPTV context data structure model. The context acquisition and transmission processes are defined, which give a guide line for the implementation. This new architecture allows the operator to provide a personalized TV service in an advanced manner, adapting the content and allowing for advanced IPTV service personalization considering rich context information related to the user daily life (user preference, location, proximity to devices, his available networks and their proximity, service context, … etc).

2) New user identification and authentication solution for IPTV service

The tight attachment of the subscriber authentication to the user equipment limits the personalization of the services. To solve this problem, a new identification and authentication mechanism using RFID and the Identity Based cryptography (IBC) is proposed, which allows service personalization through authenticating users in a personal manner during services access. Then the Open BCMP (Baskett Chandy Muntz Palacios) model is employed to evaluate the performance of the proposed authentication solution. In order to improve the performance of the authentication solution, a clustering algorithm is proposed which distributes the authentication related servers according to the service rate of the system. Through the implementation and performance analysis, the proposed clustering algorithm is proved to effectively improve the performance of the system.

3) Context-Aware Content Recommendation

Content recommendation systems should not consider only the user's preference and consumed history as the criteria, however the general context information should also be considered (like device capacity, network states, location, time, user’s activity…etc), which takes an important role for the recommendation service because the user's preference on IPTV content is not fixed and it changes depending on certain context such as time, location, activity, etc. Furthermore, certain contents are accessible based on some conditions. A new content recommendation system is proposed in this thesis, which considers not only the user’s explicit preferences but also his implicit preferences through introducing the relationship between user's watching behaviors and the context information. This makes the recommendation more accurate and personalized. This proposed recommendation system is implemented and interesting results are shown concerning the recommendation performance and accuracy.

Thesis Organization

The thesis is divided into three parts: part I focuses on IPTV personalization through chapters 1-3. Then, part II presents a user identification and authentication solution through chapters 4-5. Finally, part III focuses on a new recommendation solution based on context-awareness through Chapter 6.

In part I of the thesis: Chapter 1 gives an overview on the general concept, services, architectures aspects of IPTV and IPTV personalization. Different existing contributions that employ context-awareness as a mean to allow IPTV personalization are presented. The applications of those contributions are analyzed based upon some requirements defined for enabling advanced IPTV services personalization, and a technical comparison is proposed aiming to give some guidelines. In Chapter 2, the context-awareness principle used in services personalization is presented together with the context information that can be used in the IPTV services and the different modeling means. Also a context data structure model for the IPTV service is proposed in this chapter. Chapter 3 proposes a context-aware system for IPTV and integrates it into the IPTV/IMS architecture and IPTV/Non-IMS architecture to allow IPTV service personalization in a standard manner allowing the consideration of different context information. Implementation and the performance results are also presented in this chapter.

In part II of the thesis: Chapter 4 presents a new authentication solution for services authentication for the personalized service. The proposed solution is implemented on top of emulated GBA (Generic Bootstrapping Architecture) architecture and the performance analysis is given. Chapter 5, uses Open BCMP queuing network as a mathematical model to evaluate the performance of the proposed authentication solution. A clustering algorithm is also proposed to improve the performance of the authentication solution through distributing the servers within the architecture according to the service rate of the system.

In part III of the thesis: In chapter 6, a novel solution for content recommendation in a context-aware mean is presented allowing for customized IPTV content in an advanced mean considering each user and the different context of his environment. Implementation and the obtained performance results are also presented.

Finally, the thesis ends by the conclusion and future work presenting a summary of the research contributions carried out and indicating areas of possible future work.

Part 1 IPTV services personalization through context-awareness

Chapter 1 Background and State of the art

1.1 Overview on IPTV

Digital Television, also known as Digital TV, is the most significant advancement in television technology since the medium was created over a century ago. Digital TV offers consumers more choice and makes the viewing experience more interactive. Today, most TV operators have deployed advanced digital platforms to migrate their subscribers away from traditional TV services to more sophisticated digital services. Following the deployment of home Internet access services (digital subscriber line - based), most of the major European telecom service providers started providing triple-play (telephone, Internet access, and TV) services. One service package with video, voice, and data services is to be provided by common IP-based networks. Quadruple play also appears through adding with access to this package. Internet Protocol television (IPTV) is the process of transmitting and broadcasting television programs through the IP-based networks. A broadband connection is used as the medium of transmission for IPTV, which is very efficient compared to earlier transmission modes. From a service provider's perspective, IPTV encompasses the acquisition, processing, and secure delivery of video content over an IP based private networking infrastructure. The official definition of IPTV is approved by the International Telecommunication Union focus group on IPTV (ITU-T FG IPTV) as: «multimedia services such as television /video /audio /text /graphics /data delivered over IP based networks managed to provide the required level of quality of service and experience, security, interactivity and reliability."

1.1.1 IPTV services

Compared to traditional TV services in which all the content is pushed to the users, IPTV offers a two-way communication between operators and users. The two-way commutation capability allows service providers to deliver interactive TV applications (for example, interactive games, and high speed Internet browsing) and also allows end users to personalize their TV viewing habits by allowing them to decide what they want to watch and when they want to watch it. The following services are provided by the IPTV system [Xiao 07]:

- **Linear broadcast television:** Linear broadcast television (or live television) is the most common form of television which is similar to the traditional television broadcast provided by cable TV or satellite TV. However the distribution method is different: IPTV broadcast television uses multicast IP transport.
- **Video On Demand (VOD):** VoD services are interactive television services where the end-users select and watch video content at any point of time. The content is stored on the provider's VoD server. Clients typically have the ability to pause, play, rewind, fast forward the content, or even stop viewing it and return to it at a later time when using this service.
- **Near Video on Demand:** Near VoD is a video service where multiple copies of a program are broadcast at short time intervals (typically 10–20 minutes) on different television channels. The end users can watch the program without needing to tune in at a scheduled point in time.
- **Personal Video Recorder (PVR):** The Personal Video Recorder service is an end-user-controlled electronic device service that records linear TV and stores it in digital storage equipment, either in standalone set-top boxes or in the network. This service can support "time shifting".
- **Time shifting :** Time shifting is the recording of programs to a storage medium to be viewed or listened to at a time more convenient to the user. If the contents are stored in local hard drive, this is defined as "end-user-based time-shifting service". If the hard drives are located in the service provider's domain as opposed to the end-user's set-top box, this is defined as “network-based time-shifting service". In the network-based time-shifting service, the broadcasting traffic is transformed into on-demand traffic.
- **Multiple screens Access :** Viewing of IPTV content is not limited to televisions. Consumers often use their PCs and mobile devices to access IPTV services.
- **Session mobility service:** This service allows an on-going multimedia session to be transferred seamlessly between different devices based on user preferences.

1.1.2 IPTV versus Internet TV

Currently there are a lot of web-based video services called Internet TV. IPTV is sometimes confused with the delivery of Internet TV. Although both environments rely on the same core base of technologies, their approaches in delivering TV are different. Internet TV does not offer managed delivery of multimedia services and do not give any QoS guarantees. The video content is retrieved by the consumer using an Internet connection, without any guarantees regarding delivery, latency or availability. For instance, the popular video service YouTube offers user contributed videos on-line, but the delivery of these videos is not controlled or managed by YouTube or a related Service Provider. As the name suggests Internet TV leverages the public Internet to deliver video content to end users. IPTV, on the contrary, uses secure dedicated private networks to deliver video content to consumers. These private networks are managed and operated by the provider of the IPTV service. Furthermore, IPTV services perform the access and admission control. Before a user can use an IPTV service, authorization is used to check if the user has access rights to the content. The service will only be offered when there is sufficient bandwidth for the service (if not the service will be rejected). Using managed IP based networks and QoS guarantees leads to a distinction between IPTV services and Internet TV.

1.2 IPTV architecture

The developments of IPTV bring an entertainment revolution, where service providers worldwide consider the introduction of IPTV in their next-generation networks (NGN). In this section, we give the overview on NGN IPTV architecture. At the functional level, IPTV is mainly constituted of six functional groups. Figure 1-1, presents a high-level NGN IPTV functional overview illustrating the different functional groups [ETSI TS 182 028].

- End User Functions: Provide user connection to networks as well as control over the services. They also take charge of multimedia processing which include requesting multimedia asset in supported encoded format, decoding and presenting it to the user in acceptable format.
- Application Functions: Include IPTV and NGN application functions. IPTV applications can be regarded from two aspects: i) customer facing applications, providing service provisioning, selection and authorization of IPTV services, and ii) operator facing applications, providing operator control over IPTV subsystem in NGN,

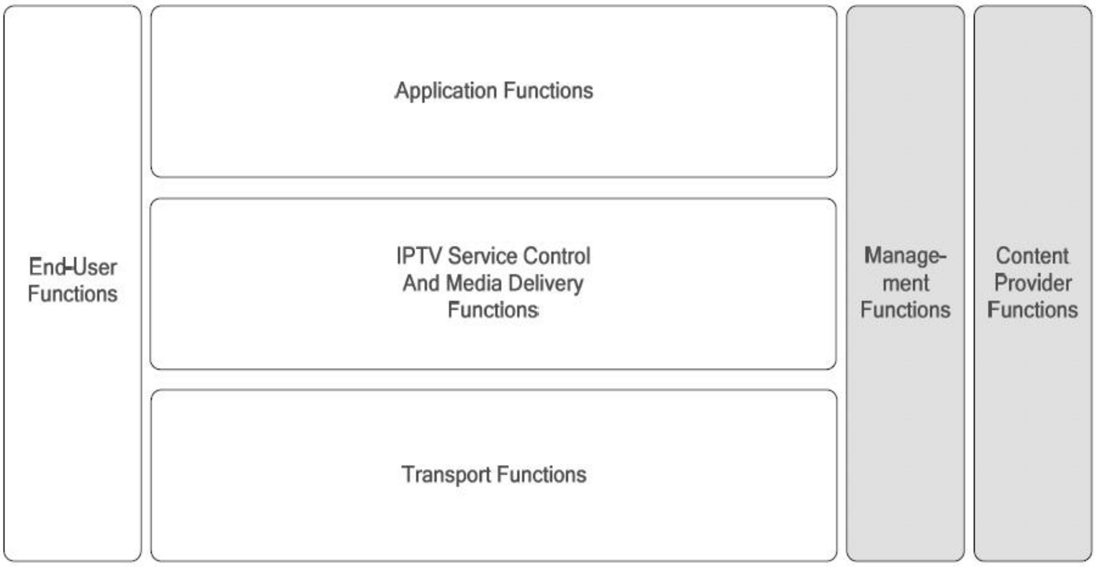


Figure 1-1: High-level NGN IPTV Functional Architecture [ETSI TS 182 028]

content preparation and media management, content licensing, and subscriber management. On the other hand, NGN applications provide the user with rich multimedia services distributed across multiple NGN subsystems, for example, messaging exchange between fixed and mobile terminals. In addition, NGN applications provide the operators with centralized NGN management interfaces to multiple subsystems for content management, charging, and interactions with others services (as IMS related services).

- IPTV Service Control and Media Delivery Functions: Enable the operation of NGN IPTV services, through taking charge of media distribution, selection and IPTV session control and management. They also manage the interactions with other NGN components for admission control as well as collecting the charging and QoS information.
- Transport Functions: Include the transport control functions which provide policy control, resource reservation, IP address provisioning, network level user authentication and access network configuration. They also include transport processing functions which are in charge of IP links and data transmission.
- Management Functions: Include the required functions to fulfil the IPTV services to the end-user, to assure the IPTV services provision, and to ensure the proper billing to the end-user for the delivered IPTV services.

- Content Provider Functions: Include the functions provided by the entity that owns or is licensed to sell contents. These are normally the sourcing of contents, metadata, and usage rights.

1.3 IPTV service personalization

1.3.1 Personalization

Personalization is the tailoring of services to individual users' characteristics or preferences and making interactions faster and easier. In a marketing environment, the purposes of personalization are defined [Bowen 04] as:

1) Better serve the customer by anticipating needs;

2) Make the interaction efficient and satisfying for the customers and service providers;

3) Build a relationship that encourages the customer to return for subsequent purchases.

User satisfaction is the objective of personalization. Personalization involves a process of gathering user-information during interaction with the user, which is then used to deliver appropriate content and services according to the user’s needs. Information about the user can be obtained from a history of previous sessions or from the interaction with the other applications in real time. "Needs" may be those stated by the customer as well as those defined by the service provider. Once the user’s needs are established, rules and techniques are used to decide what content might be appropriate. The aim is to improve the user’s experience for a service.

1.3.2 IPTV service personalization

The rapid growth of IPTV services results in enormous expansion of options for users. IPTV services provide hundreds of television (TV) channels with thousands of TV programs every day, in addition to the content available on Video on Demand (VoD) and catch-up TV stores. The amount of contents served in IPTV system far surpasses the consumption capability of consumers. Under these circumstances, recognizing what the user may like or want to enjoy becomes a challenging task for successful IPTV services. Personalization is a promising solution for this challenge. It lets IPTV services recognize a specific user, select automatically the contents that are appropriate for that user and enable the users to access and consume them in a personalized way. Moreover, the personalization of service allows providing more value added services making the IPTV service worthwhile.

Three steps are necessary to realize the IPTV service personalization, as illustrated in Figure 1-2:

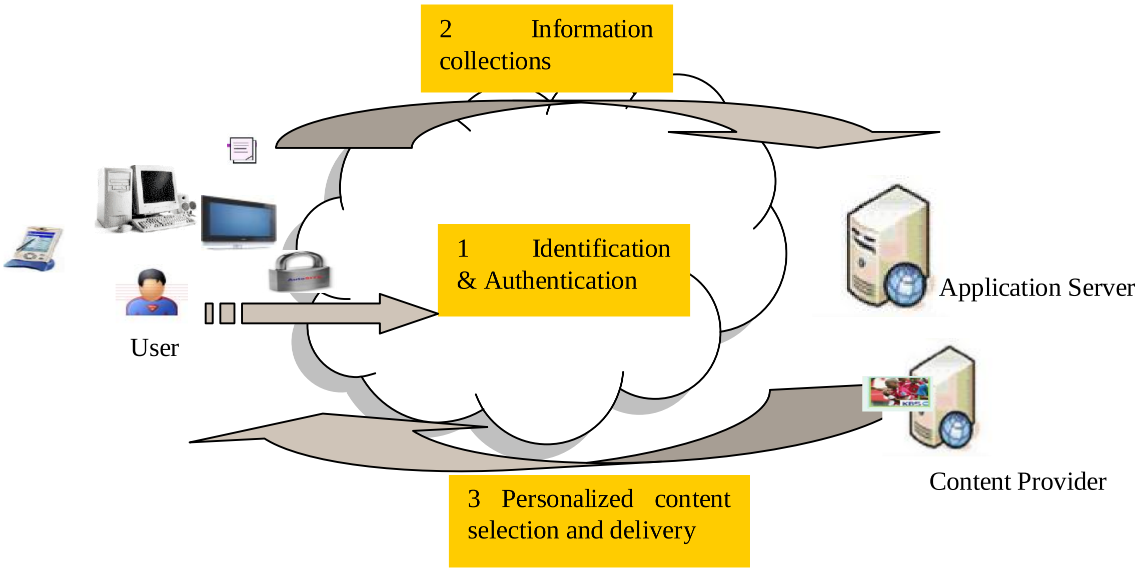


Figure 1-2 IPTV service personalization

1. User identification: To provide personalized service, the system needs to be aware of the identities of the current users in front of the TV. Different user identification and authentication techniques can be applied to IPTV system. These include biometric identification, for example speaker verification, face recognition, fingerprint; radio-frequency identification (RFID) tags; or a simple login session with user id and password.

2. Information collection: After user identification, the application server selects the personalized contents for the user. The personalized contents selection, not only need to consider the user's preferences, but also need to consider the environmental information (like device and network). For example, if a user chooses to watch TV through a terminal which does not support HD, the recommendation system should not propose the HD content for him. Also, content adaptation should be dynamically assured with the different contexts changes.

3. Personalized contents selection and delivery: According to user's preference and the environment information, personalized contents are selected by the system. The Personalized Electronic Program Guide (PEPG) is used to inform the user about all the

contents which are appropriate for him. During the content delivery, the format of the content could be automatically adapted to the capacity of network and devices. Furthermore, the notification services could be used to notify the user that a better content (more suitable for the user according to his preference or context information) is available.

Context-awareness [Schilit 94] paradigm is promising in simplifying the viewer's life, through allowing content adaptation according to the user's needs and to the surrounding environment.

1.4 Context-awareness

1.4.1 Context definition

The idea of utilizing environment information in computing systems was advocated by Mark Weiser [Weiser 91]. He first introduced the term ‘pervasive’ which refers to the seamless integration of devices into the users’ everyday life. The term “context” was first named by Schilit et al. [Schilit 94] and described as “location of use, the collection of nearby people and objects, as well as the changes to those objects over time”. Much of the early work on context-aware systems used similar extensional definitions which defined context by enumerating the constituting parameters. Brown et al. [Brown 97] enumerate “location, time of day, season of the year, and temperature”. These definitions are very special and only reflect the types of information that has been used by the researchers in their context-aware applications.

A general definition of context was proposed by Chen and Kotz [Chen 00]:“Context is the set of environmental states and settings that either determines an application behavior or in which an application event occurs and is interesting to the user.” Considering the IPTV service, context can be considered as any information that can be used to characterize the situation of an entity related to the IPTV service and to influence the working of the IPTV system. An entity could be a person, a device, or any object that is related to the interaction between a user and the IPTV service.

1.4.2 Context-Aware Application

Context-aware systems now play a very important role in modern software systems. Hull et al. [Hull 97] defined the context-aware as the ability of computing devices to detect, sense, interpret and respond to aspects of a user's local environment and the computing devices. So a context-aware IPTV application is an application which runs in an IPTV environment and which makes use of context information to provide an improved IPTV user experience. To accomplish this objective the context-aware system must:

- Gather the information from the environment or the user’s situation.
- Translate this information into the appropriate format.
- Combine or interpret context information to generate a higher context. A higher context is context information that is derived as a result of the merger of other context information or it is context information that results from interpretation of a low level context (e.g. conversion of geographic coordinates of a location received from satellite based positioning systems into street names). The main methods of context inference are logic-based reasoning and user-defined rule-based reasoning. The logic-based inference is able to infer logical consequences from a set of asserted facts or axioms. For example John is currently located in his Living Room, the context interpreter can conclude that John is located at his home since Living Room is a part of Home, logically we can infer that John is in home now. User-defined Rule-based reasoning most like patterns matching [Albin 01], in which an inference engine searches for patterns in the rules and compare with the pattern of the context.
- Store the context information and make the information accessible to other applications. There are two principal approaches of context storage and use; centralized and distributed. Centralized context storage approach provides a persistent storage for distributed context sources and guarantees integrity of context. Distributed context storage approach stores in multiple computers that are geographically dispersed and are connected via LAN or Internet to share information.
- Automatically trigger actions based on the context information and monitoring of the actions. An application discovers a change of context and adapts itself to this change (for example content adaptation service) or uses the information to change the status of other applications (for example content recommendation service).

1.5 IPTV service Personalization Requirements

This section lists the different requirements to achieve efficient and enriched personalization for IPTV services. These requirements help in evaluating the suitability and adaptability of the existing research contributions on personalized IPTV services;

1) Context-Awareness Requirements:

To generate a context-aware IPTV, the following requirements are necessary:

a) Context information flexibility and extension: For efficient IPTV service personalization, context information types should be flexible and extensible to cover the whole IPTV value chain including user domain, network provider domain, service provider domain and content provider domain. In practical, the network provider domain and service provider domain could intersect, especially in the case of integrated operators where the network provider also plays the role of the service provider. Consequently, the IPTV system should be capable of including four types of context information: i) User Context Information: presenting the information about the user, which could be static information describing the user's subscription information (ex, user's subscribed services, age, preferences, ..) or dynamic information dynamically captured by sensors or by other services (ex, user's location, agenda, available devices in his proximity, available network types and network type in use), ii) Device/Terminal Context Information: presenting the information about the devices/terminals that could be the device identity, activity status (on or off, volume), capacity, and its proximity to the user, iii) Network Context Information: presenting the information about the network such as the bandwidth and the network charge state (jitter, packet loss rate, delay, etc), iv) Content context Information: presenting the information about the content itself including the content description (content type, start time and stop time, language) and the media description (codec type, image size and resolution).

b) Dynamic context gathering and update: to allow gathering and updating in a dynamic manner the different context information on the user and his environment to be able to personalize the content accordingly.

c) Context-Awareness architectural integration: Two architectural approaches exist in context-aware systems: i) distributed context-aware systems, constituted by several distributed entities having the capacity to acquire, process, store the context information, and cooperate with each other to provide the context-aware services, and ii) centralized context-aware systems, treating and storing the collected context information in a centralized server. Distributed systems can support mobility, but they are unable to have a global view of the context information and their processing/storage capacities that are limited to the distributed terminals capacities. On the other hand, centralized systems give a global view of the context information helping nomadic service access; however the frequent and continuous communication between the devices and the server needs adequate network resources. Consequently, the IPTV architecture is required to have a hybrid context-aware system, with distributed entities to collect the context information in the local sphere and provide some simple service adaptation (for instance volume adaptation according to the environment, content transfer among different terminals), while complex service adaptation (for example the content adaptation) should be accomplished at the centralized server.

2) **Mobility requirement:** As mobile TV represents a value-added service, mobility becomes an important feature that should be supported in an IPTV system to allow the user to enjoy his personal TV content anytime and anywhere. Mobility includes terminal mobility allowing the terminal to change its location without services disruption, and session mobility allowing the user to start a media session on one terminal and to continue it on another one. Consequently, the IPTV system should be able not only to continuously collect the different context information, but also to integrate appropriate mechanisms for continuous devices discovery and continuous location discovery for the user.

3) **Nomadism requirement :** With the new model of TV systems, users should be able to enjoy their personalized TV content through any terminal. Consequently, we define a new scope for nomadism to allow each user to access his personalized TV content from any terminal not belonging to him (for instance, through the TV screen in a friend's home), though any access network (for instance, VoD in a hotel), and to pay on his own bill. Consequently, the IPTV system, besides acquiring the user identification, should also be capable of acquiring other context information as 'location, connectivity type …'.

4) **Security and Privacy Requirements:** The privacy protection is the capability of a user or group of users to secure their personal information. Since personalized service is concerned to a great extent with personal information (user context information), the privacy protection is necessary. If peoples' privacy is threatened, then services acceptability would not be guaranteed. In TV environment, the privacy protection is mainly related to the following points: controlling the personal information sharing (e.g., presence information within the presence service); not publishing the content information that the user is accessing (e.g. mastering the content sharing); user context storage and manipulation should not take place by

unauthorized entities. Consequently, IPTV systems should verify the privacy protection before any context information publishing, and should allow for the following features: group-based access control, different privacy levels (through different privacy rules), and hierarchical privacy rules (e.g. parent al control).

1.6 Existing personalization approaches and their limitations

In this section, we present some existing contributions on personalized TV and interactive TV services, which employ context-awareness in order to enhance the user interaction with the TV environment and evaluate them according to the requirements defined above.

1.6.1 Personalized Advertisement Insertion

An Application architecture for context-aware real-time selection and insertion of advertisements into live broadcast digital TV stream is proposed in [Thawani 04]. This work is based on the aggregation of past sequence of individual contexts (i.e. past viewing) and its association to the current user context in order to determine the most appropriate advertisement (ad) to be delivered relevant to the user context. The context is described as: i) location: user different locations at home, ii) identity: user identity (name, age, occupation, favorite channel or movie), device identity (screen size, required resolution), content identity (EPG “Electronic Program Guide” and other related information such as category, channel type), and event identity (information that might have an impact on the user’s watching behavior - for example, a user that doesn't like sports, during the "Olympic Games" event his viewing habit might change), iii) activity (for example user's control of the program), and iv) time. The context is stored in the Set-Top-Box (STB) constituting the user profile and is represented by XML based MPEG-7 [Martinez 04], thus enabling the determination of keywords to describe the information. The authors propose a Channel Surfing Analysis algorithm to identify the users watching the TV (acquiring his location and identity), The algorithm infers a preference list based on a dynamic analysis of the user's channel surfing activities. Then through comparing the inferred preference list with the users' preference list stored in the STB, the algorithm identifies the most appropriate user(s). However, this algorithm is based on the hypothesis that the user changes the channels according to his preferences (i.e. choosing his preferred channels), and not randomly.

This Interactive TV (ITV) architecture in this work is mainly targeting home networks and is realized by means of a middleware infrastructure having four distinct entities: User

Identification: determining which user is watching TV through the Channel Surfing Analysis algorithm; Context Derivation: a database for storing users context information; Bulk advertisement (Ad) Retrieval: acquiring ads from the operator based on the user's context information, and Context-aware Ad Selection and Insertion: responsible for comparing the user context information from the Context Derivation entity and ads from the Bulk Ad Retrieval entity to select and insert the most appropriate ads in the broadcast content.

An advantage in this work is the detection of the real user identity "who is watching TV" without introducing external objects (e.g. cameras). On the other hand, the periodic tracking and analysis of the viewing characteristics of each user, presents a limitation of this system and could not distinguish the presence of new users (or users that do not hold the remote control). We also notice that the context information treatment is realized within the STBs; and so the performance of the system is limited to the STBs processing capacity. Finally, this work does not support users' mobility and is limited to the TV screen devices while not considering the discovery of other devices according to the user location.

1.6.2 Context-Aware Interactive Television Applications

An Interactive TV (ITV) solution is proposed in [Santos 01] through applying context-awareness. Beside the context information of the user (identity, location, preference, activity, time), terminals (screen, supported content format, terminal location), and TV content (content description, video objects, program interaction), the network context (bandwidth and traffic condition) is considered.

The user context information is acquired by sensors and is forwarded to a either the STB or the user's mobile phone, which in turn processes this information. The user terminals locations are acquired by sensors while other context information of terminals (e.g. screen size, supported content format) is provided by the terminals themselves. The network related context is acquired through the "active network" principle, used to route the content according to the context (ex, traffic condition, user's location, etc.) through active nodes that process the contextual information and make a decision on the best network path to deliver the content. Finally, the content context information is provided by the content provider and is stored in the content server at the service provider or operator side.

Each physical device (STBs, mobile phones and PDAs) includes Software Agents for context treatment and storage, where each device agent discovers the other devices agents to exchange/analyze the acquired context information. Also, agents can be combined in “active nodes"; however, nothing is mentioned on how to realize "active nodes" and "active network".

The devices' capacity in discovering other devices (through their software agents) could help in supporting the mobility within the user sphere. However the lack of user identification mechanism and the distributed storage of context information stand as obstacles for nomadic TV service access. Furthermore, limited calculation capacity of the distributed agents and the lack of the dynamic user experience analysis limit the service personalization.

1.6.3 Client/Server based Context-Aware Framework

In [Moon 06], a client/server based context-aware framework is proposed to enhance the TV service through including TV Set automatic control (following the user’s commands) and personalized content recommendation functionalities (through comparing content context and user preference). In this framework, Service Agent Managers (SAM) present the client-side and sends the acquired context information to a server named CAMUS (Context-Aware Middleware for Ubiquitous System), which in turn manages this information.

The CAMUS server includes: i) a context manager that is responsible for context representation, inference and storage as well as discovering the ongoing application through receiving the service request initiated by the Service Agent Managers, and ii) a task manager having a rule-based inference engine which monitors the context manager and generates tasks according to the stored rules and ongoing applications. On the other hand, the SAM contains Service Agents that communicate with physical devices (sensors or equipment like TV Set), and notify the CAMUS when each device detects some noticeable changes and receive commands from the CAMUS to control the devices.

To carry out the automatic TV control service, the Radio-Frequency Identification mechanism (RFID) is used to identify the user and 'voice recognition’ is used to capture the user's commands. An RFID Service Agent sends the user identity information to a service publisher and the TV Service Agent receives the user's voice command, turns on the TV set and sends the context information 'TV is on' to the service publisher. This latter then sends the context information ('TV is on' and user identity) to the CAMUS server, where the context manager receives the context information, stores it into the database. The task manager monitors the database and detects that the identified user turns on the TV, so it compares the keywords of the content context with the user's preference to determine the list of the user's preferred content and activates content recommendation service.

This framework follows a client-server approach, however without mentioning where the server is located. This could allow for locating the server in the operator network or in the user domestic sphere or in a local area. This framework processes the context information on a server which has appropriate processing resources, thus helping to enhance the performance and providing implementation support. Since this framework allows the user’s identification, and with the centralized stored context information, the nomadism can be supported however limited to the server implementation scope. Although this work uses RFID to discover the users (devices) and to localize them, nothing is mentioned about the service seamless transfer, and hence the support to mobility is limited. Furthermore this work does not consider any issue on the privacy protection.

1.6.4 Personalized Recommendation TV Architecture

A context-aware based personalized recommendation architecture for Digital TV is presented in [Santos 09]. In this work, the used context information is divided into five dimensions who (identity), when (time), where (location), what (activity, the content information), and how (how can the user receive the service, through a mobile, portable or fixed device). The proposed architecture comprises a user-side subsystem and a service-provider subsystem. The user-side subsystem is implemented in the end-user terminal such as set-top-box (STB), computer or a mobile phone and includes the following modules: i) User profile manager, responsible for the acquisition of the user profile information including personal data (name, age, occupation) and user's explicit preferences (which are input manually by the user including his preferred content type, his favorite author's name, etc); ii) User context manager, responsible for the acquisition of the user's current context information like location, activity, etc; iii) User context interpreter, responsible for the inference of the implicit preference through analyzing the user current and past context information using rule-based reasoning method. The implicit preference indicates the user's current preference which may be different with the explicit preference; and iv) Recommendation manager, coordinating the other modules for the personalized content recommendation and analyzes the feedback of the user.

On the other hand, the service-provider subsystem includes the following modules: i) Context-based content filer, filtering TV programs through considering users' explicit and implicit preference, and the content description of the TV programs. ii) TV Program Description, responsible for consulting the TV programs information captured by the TV programs collector and storing it in a database. iii) TV programs collector, collecting the information relative to TV programs from outside sources such as the WEB.

When the user wants to retrieve the list of TV programs, he sends a request to the Recommendation Manager. Then the latter activates the User Context Manager to capture the user's context information (location, current time, type of access device, etc). At the same time, it requests the user profile including user's explicit preference from the User Profile Module which retrieves the user's profile from the database. The User Context Interpreter then infers the implicit user preference according to user's current context and user's profile and sends it to the Recommendation Manager. This latter forwards the implicit and explicit user preference to the Context-based Content Filter which carries out the filtering of the TV programs collected by the TV programs collector from the content sources. The filtering of the TV programs is realized through comparing the user preference with the description of the TV programs provided by the TV Program Description. Finally, the Context-based Content Filter sends the user personal TV program list to the Recommendation Manager.

When the user wants to retrieve the list of TV programs, he sends a request to the Recommendation Manager which in turn activates the User Context Manager to capture the user's context information (location, current time, type of access device, etc) and requests the user profile including user's explicit preference from the User Profile manager. The User Context Interpreter then infers the implicit user preference according to the user's current context and user's profile and sends it to the Recommendation Manager. This latter forwards the implicit and explicit user preference to the Context-based Content Filter which filters the TV programs, collected by the TV Programs Collector from the content sources, through comparing the user preference with the description of the TV programs provided by the TV Program Description. Finally, the Context-based Content Filter sends the user personal TV program list to the Recommendation Manager.

Although the user context information is stored in his devices, the personalized TV program list is returned to the user device in use without a support of session mobility from a device to another. However, personalized service access during mobility could be supported through using the user’s mobile device. The privacy protection in this work is carried out through storing the user's personal context in his devices, which is not an always practical and efficient approach, and it limits the nomadic service access through passing by other’s devices.

1.6.5 Using Smart Cards for TV Service Personalization

In [Rascioni 09], smart cards are applied to the Multimedia Home Platform (MHP) to support new interactive TV services in a personalized and secure manner. MHP [ETSI TS 201 812] is a Java based middleware designed to add interactivity to the Digital Video Broadcast (DVB) [DVB] transmission technology and integrates smart card readers and functions to connect and exchange messages with smart cards. The National Service Card (NSC) [Dhar 05] smart card type is used in this work which defines a file system architecture including cryptographic information necessary for authentication and digital signature operations, which are important for privacy protection. In this work, it is also proposed to store some user context information in the NSC. Thus, the user can use this card to authenticate to the service in order to have a personalized service access. NSC also supports different identification solutions and hence allows service access among different platforms and technologies.

We notice that this proposed solution can support nomadic and mobile personalized service access (but not session mobility among terminals) thanks to using NSC cards that are compatible with different platforms. However, due to smart card general limitation concerning the storage and processing capacity, the context information used in this solution is limited. This solution can be a good base to enhance privacy protection in personalized IPTV services.

1.7 Related standardization efforts

In this section, we present the ongoing standardization activities concerning IPTV. We also discuss the standardization activities that introduce context-awareness for multimedia and interactive applications and that could be useful for TV. For these latter, we notice that the content context information is presented by metadata that is generally provided by content providers.

1.7.1 Architecture and Services Related Standards

1) The ETSI TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networking) [TISPAN] is created in 2003 and aims to reuse the IP Multimedia Subsystem (IMS) architecture in fixed network domain. By the end of 2005, TISPAN started to develop standards for IPTV defining two IPTV solutions: an IPTV dedicated subsystem which is designed to integrate existing IPTV systems solutions with the NGN environment; and an IMS-based IPTV solution which makes use of the IMS architecture and benefits from its features (for instance user and network authentication, user profile, charging and so on). The IMS-based IPTV solution also allows blending the TV services with other

Telecommunication services like messages, presence, and several innovative and convergence services (where some of them are still under specification as: Caller ID on TV, Virtual Living-Room, etc).

2) The ITU-T (International Telecommunications Union – Telecommunication Standardization Sector) [ITU-T] established a Focus Group on IPTV in 2006 with an objective to coordinate and promote the development of global IPTV standards taking into account the existing work of the ITU study groups as well as that of other standardization. The ITU-T IPTV Focus Group describes the basic IPTV services and provides three possible options for IPTV architectures: an architecture for non-NGN network components, an architecture based on the NGN functional architecture, but not based on IMS and an architecture based on NGN and its IMS component. Some personalized IPTV services are defined in the ITU:

- Personal video recorder (PVR): is an end-user-controlled electronic device service that records linear TV and stores it in a digital storage facility, either in standalone Set-Top-Boxes (STB) or in the network.
- Personal Broadcast Service: is a service providing the end-user with a way to advertise personal content (possibly including scheduling information) description so that other users can access such content. The service provider is responsible for relaying session information between the broadcasting and receiving end-users, possibly assuming some access control functions.
- Targeted Advertising: is a commercial advertising or public promotion of goods, services, companies and ideas, usually personalized according to the end-user's preferences or centers of interest, based upon the end user's profile characteristics in order to match the audience with the campaign objective requirements.
- Presence services: managing presence information between each end-user and other users or any service making use of the presence information of users. Example of services might include: personalization based on presence on top of locally stored data, targeted advertising correlated with time of day, and chatting with friends watching the same channel.

3) The DVB-IPTV [DVB-IPTV] is a specification developed by the Digital Video Broadcasting (DVB) [DVB] to facilitate the delivery of digital TV services over IP networks. The initial phase of DVB-IPTV's work is to specify the technologies of the interface between the IP network and a Home Network End Device (HNED), for example the Set-Top-Box

(STB). On the other hand, the DVB project designs an open middleware system standard called Multimedia Home Platform (DVB-MHP) [ETSI TS 201 812] for interactive digital television, where the DVB-IPTV also provides additions to the DVB-MHP middleware specifications to allow the MHP to support interactive TV application in DVB-IPTV environment.

4) The Open IPTV Forum [Open] was founded in March 2007 with the purpose to provide an end-to-end solution for supplying IPTV and internet multimedia services. The function domains of the designed architecture cover consumer, service provider, network provider and content provider. The Open IPTV standard follows two business models: Managed Network model and Open Internet model. In the managed network model, the operator provides IPTV services, operates the service platform and delivers the services through the operator's access network. The IMS is selected as the enabling architecture for the Managed Network model. In the Open Internet model the services are delivered over the public internet. User profile management: refers to the set of operations that allow a user to manage his profile, including the ability to create, retrieve, modify, delete, or replace the profile.

1.7.2 Internet Protocols Related Standards

Session Initiation Protocol (SIP) [Rosenberg 02], is defined by the Internet Engineering Task Force (IETF) [IETF], as an application layer control protocol for creating, modifying, and terminating sessions. This protocol is widely used in the IMS architecture. SIP has some support for expression of capabilities information like Accept-Language, but very limited. Furthermore it does not provide a general framework for expression of capabilities. User Agent Capabilities in SIP [Rosenberg 04] are now being discussed at the IETF in draft forms under progress. This work provides a more general framework for describing the capabilities and characteristics of user agents in SIP, where the information about capabilities and characteristic is carried as parameters of the Contact header field. The work in [Lonnfors 08] enables SIP presence implementation to represent User Agent Capabilities within presence information.

1.7.3 Context-Aware information Related Standards

Within the World Wide Web Consortium (W3C) [W3C], the Composite Capability/Preference Profiles (CC/PP) [Kiss 07] specification was developed for describing device capabilities and user preferences aiming to guide the adaptation of content for each device. CC/PP is based on the Resource Description Framework (RDF) [Klyne 04], which was also designed by the W3C as metadata description model. A CC/PP profile is constructed as a

2-level hierarchy, in which a profile has at least one or more components and each component has at least one or more attributes. The attributes names and associated values are used by a server to determine the most appropriate form of content to deliver to the client. On the other hand, the Wireless Application Protocol (WAP) Forum [WAP] developed the User Agent Profile (UAProf) [WAG] as a specification related to CC/PP, but more specified for mobile devices. UAProf defines a profile file named Capability and Preference Information (CPI) containing the information like hardware characteristics, software characteristics, application/user preferences, and network characteristics. This information is conveyed between the mobile terminals and the servers and help to adapt the content.

As previously discussed, under the IETF, the Presence Information Data Format (PIDF) [Sugano 04] is used as a protocol header to describe a basic presence information data format presented through XML for exchanging presence information. The exchanged presence information includes a Uniform Resource Identifier (URI) for communication, an indication of availability (open or closed) of the URI owner and a textual note that can be given by this latter. Due to the limited PIDF information, a Rich Presence Extensions to the Presence Information Data Format (RPID) [Schulzrinne 06] is also proposed at the IETF to convey richer presence information about the presence entity (URI owner) and its different contacts (other URI owners), for example what the person is doing, the person's mood, the type of place a person is present, when a service or device was last used, etc.

1.7.4 Content Metadata Related Standards

1) MPEG-7 [Martinez 04] is an ISO/IEC standard developed by MPEG (Moving Picture Experts Group) [MPEG], formally called Multimedia Content Description Interface. MPEG-7 uses a standard language called Description Definition Language to represent specific low-level features of the content, such as visual (e.g. texture, camera motion) or audio (e.g. melody) features and also metadata structures for describing and annotating the content. The metadata structures are composed by a set of related low-level features, allowing the user to find the content that interests him in an efficient way. On the other hand, MPEG-21 [Bormans 02], also called Multimedia Framework, defines an open framework to enhance the management of digital media resources exchange and consumption. It aims to achieve the functions such as digital content creation, distribution, user privacy protection, terminals and network resource extraction.

2) TV-Anytime [TV-Anytime] is developed by the TV-Anytime Forum and provides metadata to assist in the delivery of multimedia content for the user's digital video recorder (DVR). The TV-Anytime Metadata Specification allows describing segmented content, where Segmentation Metadata is used to edit the content for partial recording and non-linear viewing. Another important set of metadata consists of describing user preferences, representing user consumption habits, and defining other information (e.g. demographics models) for targeting a specific audience, which is useful in content recommendation and targeted advertisement.

1.8 Conclusion

In this chapter an introduction on IPTV was presented, discussing the general IPTV service and also IPTV architecture in NGN environment. IPTV allows TV services to evolve into true converged services, blending aspects of communications, social media, interactivity, non-linear TV and search and discovery in new ways. These efforts address the growing consumer desire for personalization and customization of TV experiences. Context-awareness is promising in enhancing the IPTV system through appropriate service personalization ranging from users' interactivity and content adaptation to providing smart and advanced services.

Through the study and analysis for the different related contributions, it is noticed that the existing contributions could not satisfy IPTV services personalization in a complete and adequate manner. And the existing IPTV services are limited to the home sphere and no existing contribution focuses on the architecture of the context-aware IPTV from the operator's point of view. Furthermore, the privacy protection is another issue that is not resolved in the existing contributions, although user-context information should not be a way that threatens the user privacy.

The following table gives a summary and comparison on the discussed contributions and their support to the different personalization requirements discussed before in this chapter in session 1.5.

Table 1-1: Technical Comparison of the different contributions

	Context information domain	Distributed (D) centralized (C) or partially-centralized (PC)	The context information extension	Support for mobility	Support for nomadic	Support for privacy protection	Performance and feasibility of implementation	Support personalization	Co-existence of multiple actors
Personalized Ads	+	PC	-	-	-	-	-	+	+
Interactive television	++	D	+	+	-	-	-	-	+
Client/Server based	+	C or PC	+	-	+	-	+	+	++
Personalized TV	+	C	-	+	+	+	+	+	++
Smart Cards	+	D	-	+	+	++	-	-	+

'-': not supporting the requirement, '+': partially supporting the requirement, '++': well supporting the requirement

Chapter 2 Context information types and modelling for IPTV service

Context-aware systems now play a very important role in modern software systems. A context-awareness IPTV makes use of context information to provide an improved IPTV user experience. This chapter describes the context information used for the television services showing their types and modeling means.

2.1 Context information for IPTV services

The ITU-T defines four main functional domains involved in the provision of an IPTV service as illustrated in the Figure 2-1:

- Content Provider: This entity owns or sells the content to be streamed to the Customer.
- Service Provider: The IPTV service is provided by the Service Provider; the content is licensed or acquired from the Content Provider. The Customer buys the service which is a package that the Service Provider creates from the available content.
- Network Provider: The connection between the Service Provider and the Customer is assured by the Network Provider.
- Customer: This entity purchases and consumes the IPTV service.

From the IPTV function domains, four types of contexts can be defined for IPTV services: 1) User Context, 2) Device/Terminal Context, 3) Network Context, 4) Service Context:

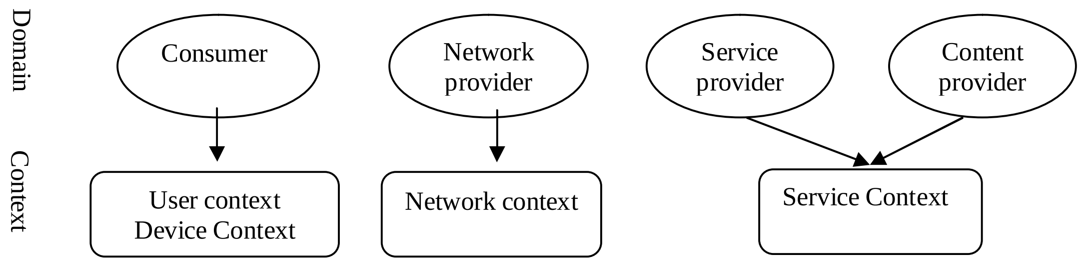


Figure 2-1 IPTV service domain and context type

The four context categories cover all the context information types which can be used for any IPTV application to improve its services. For each of context type, context sources and context acquisition functions are used to collect the information which is needed to form a context- aware service. Context information can be combined to derive higher level context information which is very useful in the application point of view. This combination can be done using various reasoning engines or different kinds of context information.

2.1.1 User context information

User Context information includes information about the user which could be static information, dynamic information and inferred information.

1) Static information describes the user's personal information which does not change for a long time and stored in the database, including user's profile (identify, name, age, and gender), user's static preference (preferred audio/subtitle language, favorite content genres, favorite actors, favorite director). This information is explicitly indicated by the user during the service subscription. Most recommendation services employs the user's static information to select the most proper contents for user [Yu 03, Chen 09].

2) Dynamic information presents the context information that changes frequently, including user's location, agenda and user's emotion. The dynamic information makes the IPTV service adapt to the user's situation at a given moment and achieve the better quality of experience. For example, content recommendation decisions can also be made by looking at the user's calendar information. It is not required to provide a recommendation of watching a movie which is three hours long when user is scheduled to be out in one hour. TV experience can be enhanced by personalizing it during special occasions like birthdays and public holidays. From detecting the user's position in the room, IPTV system could switch the content to the terminal which is near to the user. The dynamic information is captured by sensors or by other services. Emotion can easily be identified if the IPTV has a camera attached to it by using face recognition. Also voice sensors can help identifying emotions. There are lots of technologies that can be used to detect user location including indoor location and outdoor location. For indoor location, we have RF radio signal (WI-FI signal, Bluetooth) technology based localization, vision based indoor localization (using camera), etc. For the outdoor location, GPS is frequently used technology, because currently all smart phones at the market are capable of receiving GPS signal and providing coordinate information.

3) Inferred information is high-level information which is difficult to be acquired directly from the sensors however it could be acquired through analyzing or combing other

context information. User’s action is a kind of high-level information. User’s experience can be enriched if the activity of the user can be identified. Through detecting the user's actions, IPTV system can realize automatic control. For example, when the user enters a room, the IPTV can switch ON automatically. And if the user goes into the kitchen and prepares the dinner (ex, user's action “user is going to the kitchen' is inferred by the changed location, user’s action ‘prepare the dinner’ is inferred by a series of actions: enters kitchen, opens the refrigerator, takes out the vegetables …), an advertisement regarding the food stuff can be selected and shown on the TV screen in the kitchen. Other important inferred information is user’s watching habits which indicate user’s repetitive actions such as watching news every evening and watching a movie at the bedroom. User’s watching habits is inferred from the consumption history and used to improve the accuracy about the recommendation service.

2.1.2 Device context information

User can access the multimedia content through various devices which may have different device’s screens size, capacity (hardware, supported content format), connectivity (which determines the network connectivity like GPRS, 3G, Wi-Fi) as well as status of the devices (turn on or off, volume). The IPTV system could benefits from the device context information to select the content and adapt the format of the contents to the device. For example, if a device has a small screen and only supports the standard definition format (SD), the IPTV system can filter out the contents that do not meet the conditions. Furthermore, knowing the device’s location and the device proximity with respect to the user, the IPTV system can provide the location based recommendation service. Other useful information is about the mobility of the device, like mobile phone and tablet. If user starts using television while watching TV, when he leaves room with a smart phone, he could continue watching the content though his smart phone.

Other devices such as laptops, music station can also be connected to a TV and display the content on nearby screen. Protocols like LLTD [Link], LLDP [IEEE 802.1], UPnP [Universal] and DLNA [Digital] could be used. A useful example is that: the photos which are stored in the laptops could be displayed on TV.

2.1.3 Network context information

Network context information represents the characteristics of the access link being used for accessing TV content. Transport networks and their states directly affect means to access content, content presentation (especially quality), and also user experience, e.g. for an interactive content where low latency is an important prerequisite. Network conditions are variable and must be taken into account by the content adaptation service. Network context information includes

- Access network type: Information about available access networks enables selecting the most appropriate network.
- Available link bandwidth: this information is used by the IPTV system to select appropriate content format for example SD or HD.
- QoS information: this information is used to monitor the state of the network. This information can be acquired during the content delivery from the RTCP (Real-Time Control Protocol) report [Schulzrinne 03], for example information about jitter, delay and packet lost.

2.1.4 Service context information

Service Context presents the information about the service and includes content description and capacity requirements.

- Content description is used to provide general information about media content, such as title, keyword, director, actor, genre, description, content duration and language. IPTV system uses this information to match user preferences to select the contents that user might be interested in. This information is contained in the Electronic Program Guide (EPG) [DVB 11].
- Capacity requirements describe the media itself, including the codec format (for example MPEG2, MPEG4 , AVC or AVS), resolution (High Definition or Standard Definition), minimal bit rate requirement, and required latency. Such information enables to select the most appropriate device and access network. For example, the table below presents the Recommended Minimum Transport Layer Parameters for Satisfactory QoE for different codec format and resolution defined in ITU [ITU 08].

Table 2-1 Recommended Minimum Transport Layer Parameters for Satisfactory QoE [ITU 08]

Codec	Resolution	Transport stream bit rate (Mbit/s)	Average IP Video Stream Packet Loss Rate
MPEG2	SD	3.0	<= 5.85E-06
MPEG4	SD	1.75	<= 6.68E-06
AVC	SD	2.0	<= 7.31E-06
AVS	SD	2.5	<= 5.85E-06
MPEG2	HD	15	<= 1.17E-06
MPEG4	HD	8	<= 1.28E-06
AVC	HD	10	<= 1.24E-06
AVS	HD	12	<= 1.22E-06

2.2 Context Modelling

Context models are used during contextual information acquisition, storage and retrieval. A good model does not only provide ways for effective contextual information retrieval, but also effective processing of such information. Effective deployment and easy utilization of context-aware system is also determined by context models. Recently, various context management and modeling approaches have been introduced. Strong and Linnhoff-Popien [Strong] summarized the most widely used data structures. They are Key-Value-Pair modeling, Graphical modeling, Object oriented modeling, Markup scheme modeling, and Ontology.

Key-Value-Pair modeling is the simplest data structure for context modeling and easy to implement and use, and they are frequently used in various service frameworks. This model is powerful enough to allow pattern-matching queries, but is not efficient for structuring purpose and not suitable for applications with complex structures. Schilit et al [Schilit] models the contextual information in a key-value pair, with an environmental variable acting as the key and the value of the variable holding the actual context data. Graphical modeling is particularly used to model contextual aspects. The strengths of graphical models are on the structure level. They are mainly used to describe the structure of contextual knowledge (the objects and their relationships) and derive some code from the model. But they are usually not used at instance level. The Graphical modeling is always based on the Unified Modeling Language (UML) [Booch 00].Object oriented modeling possess the main benefits of any object oriented approach. They encapsulate all the details of data collection, data fusion and context processing within the active objects. The context information is accessed through well-defined interfaces, and can be reused. These characters make object oriented models strong regarding distributed composition. And the propriety inheritance makes applications easier to define the objects and theirs relationships. The key problem with this approach is that the represented information lacks expressiveness and extensibility. And these models have usually strong additional requirements on the resources of the computing devices which often cannot be fulfilled in ubiquitous computing systems. Markup scheme modeling uses standard markup languages or their extensions to represent context data. A mark-up language uses a set of symbols including "vocabulary," "grammar" and “syntax" to describe the text, image or other form of data. The most widely used markup languages is XML which is used for identifying the content of the document. In the markup context models, contexts are modeled as tags and corresponding fields. Ontology based models use ontology and related tools to a description of the concepts and their relationships. An ontology is a "formal, explicit specification of a shared conceptualization" [Thomas 93] An ontology renders shared vocabulary and taxonomy, which models a domain with the definition of objects and/or concepts, and their properties and relations [Arvidsson 08]. Therefore, ontology is a very promising instrument for modeling contextual information due to their high and formal expressiveness and the possibilities for applying ontology reasoning techniques. The following subsection presents these standard information model solutions, and then a proposed data structure for the context-aware IPTV service is presented which extends the standard structure to support more context information.

2.2.1 Markup modeling based metadata for the content description

The current IPTV services are focused on delivery of the audiovisual contents. In order to easily find, navigate and browse the IPTV contents, IPTV service use metadata to can provide rich information about the program contents such as program title, genre, synopsis, actors/actresses, copyright information, production date, emission date etc. Metadata is defined as data that describe other data, and can provide insight into syntax and semantics of complex data. Markup schema modeling is designed for the processing, definition and presentation of text and is very suitable for the metadata description. MPEG-7 [Martinez 04] and TV-Anytime [TV-Anytime] are well-accepted standards which provide structured metadata for the description of the audiovisual content.

A) Mpeg 7

The MPEG-7 descriptions are used in any audiovisual digital library environment or any other audiovisual web application environment to describe audiovisual content and user preferences. Such descriptions of media help users or applications to identify, retrieve, or filter audio–visual information. Examples of applications include broadcast media selection (e.g., personalized radio, TV channels), digital libraries (image catalog, musical dictionary), multimedia directory services (e.g., yellow pages), and multimedia editing (e.g., personalized electronic news service, media authoring).

MPEG-7 standard provides a set of multimedia description tools to generate descriptions. The basic elements include data types, vectors, matrices, and constructs for linking media files, localizing pieces of content, places, time, persons, individuals, groups, organizations, and other textual annotations.

To create descriptions, MPEG-7 offers a set of audio visual metadata elements including Descriptors (Ds) and Description Schemes (DSs) and Description Definition Language (DDL). Ds define syntax and semantics of features of audio–visual content. Different levels of abstraction are addressed by MPEG-7. At the low abstraction level, Ds may include shape, motion, texture, color, and timbre for audio. At the high abstraction level, Ds may include events, abstract concepts, content genres, etc. DSs allow construction of complex descriptions by specifying the structure and semantics of the relationships among the constituent Ds or DSs. MPEG-7 also includes information about the coding scheme used for compression of content (e.g., JPEG, MPEG-2). The DDL allows flexible definition of MPEG-7 DSs and Ds based on XML Schema, providing the means for structuring the Ds into DSs. Figure 2-2 shows a relationship between the different elements.

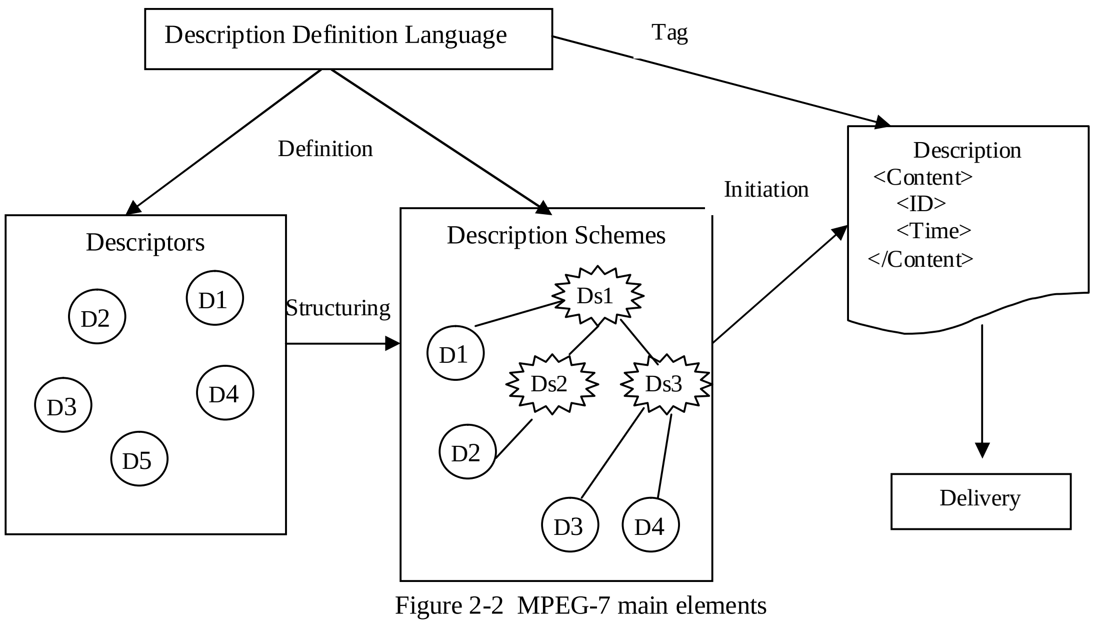


Figure 2-2 MPEG-7 main elements

B) TV-ANYTIME

The TV-Anytime is an open standard with a set of specifications defined by the TV-Anytime Forum founded in 1999 by major companies seeking to develop a set of specifications that enable electronics manufacturers, content producers, service providers and users to exploit the high volume of content on devices with digital storage capacity. This forum has produced specifications that include segments related to the business model, system architecture, metadata, reference to content and copyright management.

The TV-Anytime metadata system defines a standard way to describe consumer profiles including search preferences to facilitate automatic filtering and acquisition of content by agents on behalf of the consumer. For the purpose of interoperability, the TV-Anytime Forum adopts the XML-based MPEG- 7 Description Definition Language (DDL) as a format for representation of metadata, and the XML Schemas for the formal definition of the structure and syntax of metadata. The TV-Anytime metadata contains following basic elements:

- Content description metadata contains the descriptions of items of content e.g. television programs. These descriptions are held in the ProgramInformationTable and include things like the title of the program, a synopsis, the genres it falls under and a list of keywords that can be used to match a search.
- Instance description metadata contains the information about the scheduled time and also the duration. This information is held in the ProgramLocationTable.
- Consumer metadata contains the details of a user's preferences and user’s usage history. The user’s preference information is delivered by the UserPreferences description scheme, which provides rich representations of the particular types of content preferred or requested by the user. These descriptions are closely correlated with media descriptions, and thus enable users to efficiently search, filter, select and consume desired content. The user’s usage history is described by UsageHistory description scheme which provides a list of the actions carried out by the user over an observation period. This information can subsequently be used by automatic analysis methods to generate user preferences.

2.2.3 Graphic modeling based IPTV user profile structure

ETSI/TISPAN defines the IPTV service relevant IPTV User Profile structure [ETSI TS 182 028] that encompasses the information required by user to operate an IPTV service including services (Broadcast, CoD, PVR) setting, user setting and global setting.

- The service setting contains a set of the service packages. Each service package is a set of elementary TV services, along with a description (service metadata). The service setting also includes a quality definition level (e.g. standard or high definition or other defined quality level). Delivered quality level depends on this quality definition level as well as user equipment (UE) capabilities, available codec and/or bandwidth limitations.
- User setting: includes information related to the capabilities of the UE(s) that an IPTV user is associated with. An IPTV user may be associated with one or more UE(s) and every UE is uniquely identified with a unique UE Identifier (UE ID).
- Global settings contain the information about preferred languages which could be used to configure the subtitles. The parental Control information is also contained in the Global setting.

The User profile structure does not cover all information related to the user and currently contains only the critical information for the IPTV services. Most information presented in the user profile structure is the static information. This structure does not contain the dynamic information which is very important for the content personalization and service adaptation, for example, the location of the user. The next subsection presents an IPTV data structure proposed in this thesis based on the TISPAN standard structure however contains more information for more enrich IPTV services.

2.2.4 Proposed Graphic modeling based IPTV Context data structure

A graphic modeling based structure for the context-aware IPTV service is proposed in this subsection and shown in Figure 2-3. This data structure defines a number of classes and attributes. This structure models the context information used for the IPTV services which cover all the IPTV service chains: user, device, network and service.

(1) User context modeling

The “User” class defines typical description for a person. Besides the profile description, there are specific information about user’s preference, locations, behavior, and consumption history.

Profile: The profile reflects user's static personal information including attributes like "Name", "Gender", "Age", "Occupation" and "Preferred Language".

Preference: The preference reflects user's preference. The attribute "HasPreference" lists all the user defined preferences. The metadata used to describe the user's preference is following the same structure defined in the TVAnytime.

Consumption history: Models and stores user's consumed content information. The attribute "ViewedContent" describes the characteristic about the consumed content. The attribute "HasContext" describes the context situation in which the content is consumed. The value of this attribute could contain all the related context information including: location, time, used devices, etc.

Location: The location of a user is modeled in several ways in response to varied references. The attribute "LocatedIn" denotes a user located in a room and the attribute "LocatedNear" represents a user's location nearby a certain device.

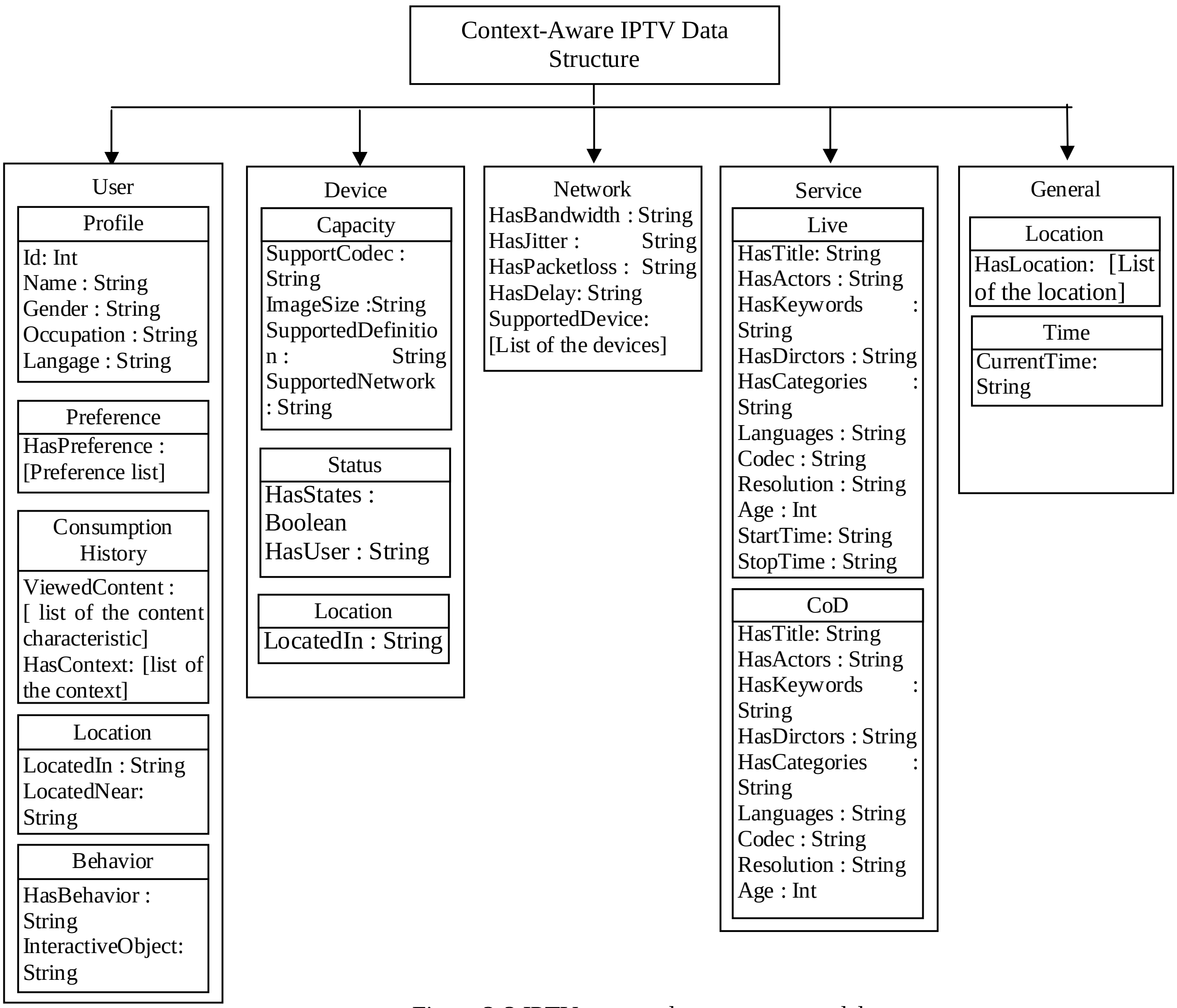


Figure 2-3 IPTV context data structure model

Behavior: Describes and models the user's behavior which is used by the IPTV system to adapt the service. For example, when the user is receiving a telephone call, the IPTV system makes the TV into mute mode or display the telephone number on the screen. The attribute "HasBavior" denotes the user's behavior which will influence the IPTV service. The attribute "InteractiveObject" denotes the object with which the user interacts. For example, user's behavior "watching TV from a Television", has an interactive object "television".

(2) Device Context modeling

The "Device" class defines the description for a device, including the capacity characteristic, status, location.

Capacity: Contains the capacity information about the devices which will be used by IPTV system to select or adapt the content. The attributes "SupportCodec", "ImageSize", "SupportedDefinition", "SupportedNetwork"are contained in this class.

Status: This class contains the actual usage about the device. The attribute "HasStates" reflects whether the device is power on. The attributes "HasUser" denotes the user who is using the device and establishes the relationship between the device and user.

Location: The attribute "LocatedIn" of this class helps the IPTV system to find the nearest device for the user.

(3) Network Context modeling

The "Network" defines the description for a network, including the network situation. The attributes "HasBandwidth", "HasJitter", "HasPacketloss", "HasDelay" present the state the network information. The attribute "SupportedDevice" denotes which device supports the network and establishes the relationship between the device and network.

(4) Service Context modeling

The "Service" class defines the description for a service. The services LIVE, VoD defined as the subclass of the class "Service". Each subclass contains the following attributes "HasTitle", "HasActors", "HasKeywords", "HasDirctors", "HasCategories", "Languages", "Codec", "Resolution" and "Age". For the LIVE, the attributes "StartTime" and "StopTime" give the information about the start time and stop time. The structure and description of the service information benefit from the existing structure and metadata representation in TVAnytime and MPEG-7.

(5) General Context Modeling

Besides User, Device, Service and Network Context, class “General” is proposed which describes the general context information, for example the information about possible location for the user (all the rooms in the house); the current time, etc.

Location: This class presents the possible location for the user in the house, for example kitchen, bedroom, salon, etc. The attribute “HasLocation” lists all the rooms in the house and gives an ID for each room which will be used in the User Class and Device Class.

Time: This class contains an attribute “CurrentTime” and gives current time.

The context data architecture gives the diagram with the main class and also the attributes that present the context information used in the IPTV services. For the representation of context the markup language (XML) based format is adopted in this proposed model, for reasons of interoperability and ease of integration with the descriptors and description schemes patterns of TV-Anytime metadata and MPEG-7 metadata. The XML document defines a hierarchical structure which helps to present the different context information levels about a service, a device, or a person and to derive more information. Another important reason is that XML files can be easily integrated into the transport protocol like SIP and HTTP.

2.3 Conclusion

Context-awareness through the exploitation of context enriches the user experience in television, especially when used in interactive applications to provide content in a personalized way. This chapter discusses the context information that can be used in the IPTV services and the different modeling means. Also a context data structure model for the IPTV service is proposed in this chapter. This proposed model helps the context representation and simplifies the context information transmission which will be used in the context-aware system proposed presented in the next chapter.

Chapter 3 Personalized IPTV through context-awareness

The Next Generation Network (NGN) approach in coupling IPTV with IP Multimedia System (IMS) and allows for services convergence through using the IP Multimedia Subsystem (IMS) common architecture in providing a platform for interactive TV services. Although the rapid advancement in interactive TV technology (including IPTV and NGN technologies), choosing the desired channel in a manual means could disturb the viewer. IPTV service personalization is still in its infancy. Personalizing the IPTV services according to the user's context and his environment context (devices and network) still presents a challenge. Context-awareness is promising in allowing services personalization through considering the context of the user and his environment (devices and networks) as well as the context of the service/content itself. Through context-awareness, users can transparently interact with the IPTV system (users will no longer be required to give explicit instructions at every step while watching TV). Context-aware IPTV could provide services dynamically optimized taking into consideration the user contexts as well as the content and adaptation needs. This chapter presents a proposed context-aware IPTV system which extends the existing IPTV system through the integration of a context-awareness system. This new IPTV system allows network operators and service providers to offer personalized TV services in an advanced manner, adapting the content according to the context of each user and his environment.

3.1 Existing IPTV architecture

3.1.1 IPTV IMS architecture

The functional architecture of IMS-based IPTV contains main functions defined in ETSI TISPAN IMS-based IPTV architecture (including service control functions, media control functions, and media delivery functions).

As shown in Figure 3-1, the user equipment (UE) can communicate with the IPTV application servers (including service control functions) over various interfaces for different purposes, namely, over a Gm interface via the IMS core for the session management purpose, directly over a Ut interface for the service profile configuration purpose, or over the Xa interface to interact with service selection functionalities. The IPTV application server functionality uses the IMS service control (ISC) interface to communicate with the IMS based NGN service control functions. Media control functions (MCFs) can control media delivery functions (MDFs) over an Xp reference point that enables the building of a scalable and distributed media delivery infrastructure. External content can be imported from external media sources (e.g., the content providers or IPTV head end) by an external interface to the MDF.

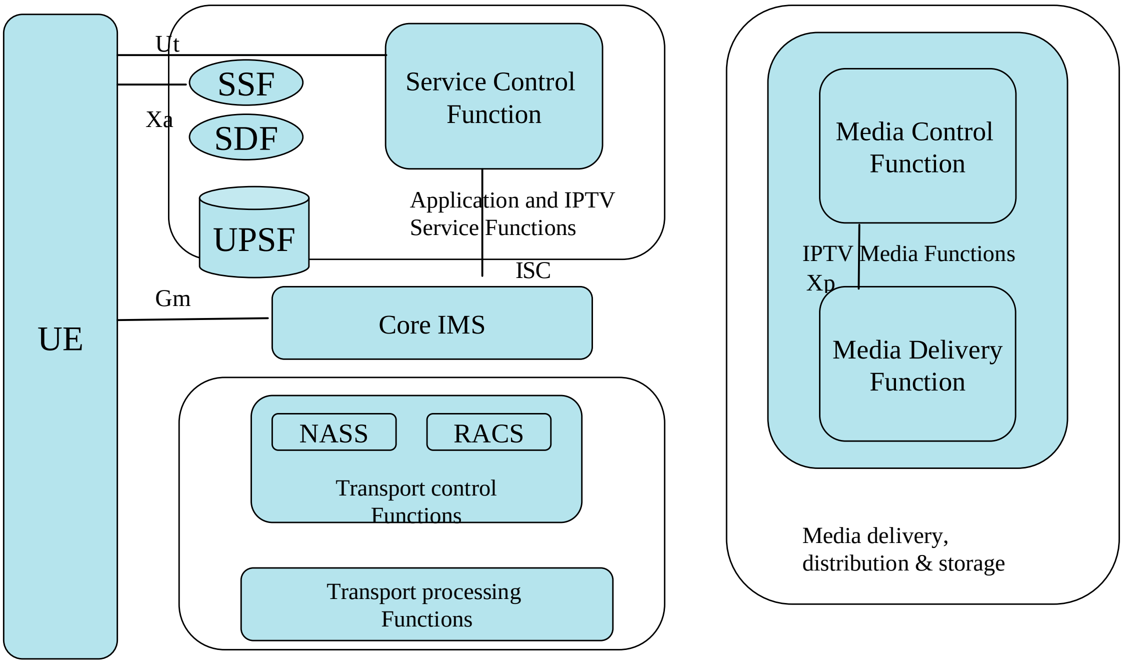


Figure 3-1: IMS IPTV Functional Architecture [ETSI TS 182 027]

(A) IMS CORE

IP Multimedia Subsystem (IMS) [Camarillo 06] is an open and standardized architecture for mobile and fixed services. It was originally designed by the 3rd Generation Partnership Project (3GPP) wireless standard body [3GPP] and was later extended by the ETSI TISPAN standard body as a subsystem of Next Generation Network (NGN). IMS supports IP Multimedia applications such as video, audio and multimedia conferences where the Session Initiation Protocol (SIP) protocol was chosen as the signaling protocol for creating and terminating Multimedia sessions. The media flows of established sessions like IPTV streams, do not traverse the core IMS. Since IMS uses SIP for the control and signaling of sessions, its main architectural elements are constituted of SIP proxies, known as Call Service Control Functions (CSCF), which are introduced to establish a multimedia session between subscribers and to prepare delivery of the demanded services according to the session characteristics required by users. Some of the CSCFs have interfaces to the home subscriber server (HSS) where the complete information about particular subscribers is stored, such as their user profiles, policies, subscriptions, preferences, and so on. Figure 3-2 illustrates the main entities constituting the IMS core architecture. The CSCFs handle all the SIP session signalling and are classified into P(proxies)-CSCF, I(interrogating)-CSCF and S(serving)-CSCF.

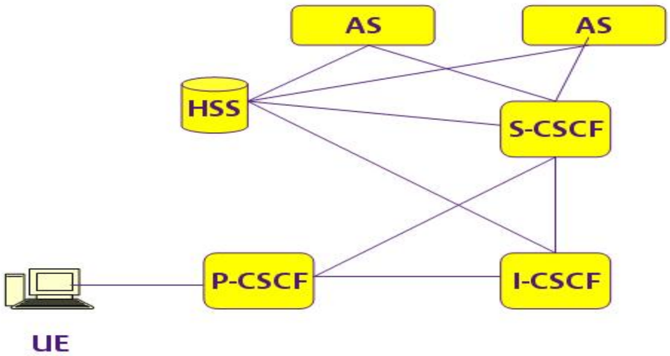


Figure 3-2 IMS architecture

- P-CSCF is used as the IMS contact point for IMS end users. The main goals of the P-CSCF are the guarantee of signalling messages between the networks and subscribers and the resource allocation for media flows by interaction with the resource and admission control subsystem (RACS) defined in TISPAN.
- CSCF presents the contact point within the operator's network and forwards connections to the appropriate destinations. It queries the HSS to discover the appropriate S-CSCF for the subscriber. It also can be used to hide operator network topology from other networks.
- S-CSCF is considered as a focal entity in IMS. It processes registrations from subscribers and stores their current location and also is responsible for subscriber authentication and managing the application servers (AS).
- The Home Subscribe System (HSS) is another important entity in IMS which is a database for all subscribers and service-related data for IMS. The main data stored in the HSS includes user identities, registration information, etc.

During the user registration, firstly the P-CSCF contacts the I-CSCF for acquiring the address of the S-CSCF corresponding to the user. The I-CSCF in turn contacts the HSS to assign an appropriate S-CSCF and forwards the registration request to it. When the S-CSCF receives the registration request, it downloads the user's authentication data from the HSS and based on such authentication data, it generates a challenge to be sent to the end user/UE (User Equipment).

(B) SERVICE DISCOVERY AND SELECTION

The Service discovery function (SDF) and the service selection function (SSF) provide the information that is required for a UE to select an IPTV service. The SDF is responsible for providing service attachment information about accessible IPTV services (service discovery). In IMS-based IPTV, one or several SSFs are used to provide service information including electronic program guide (EPG) or service program guide, as well as information about media delivery.

(C) IPTV SERVICE CONTROL FUNCTIONS (SCFs)

IPTV SCFs handle IPTV-related requests and execute service and session control for all IPTV services. These functions are also responsible for interworking with the IMS core on the service control layer. General tasks of an SCF are summarized as follows:

- Session initiation and service control for IPTV services.
- Interaction with the IMS core and S-CSCFs to receive, validate, and perform IPTV service requests from users.
- Service authorization and validation of user requests for selected content, based on the user profile information.
- Selection of the relevant IPTV media control/ delivery functions.
- Accounting and billing.

(D) IPTV MEDIA FUNCTIONS

IPTV media functions include Media Control Functions (MCFs) and Media Deliver Functions (MDFs). The IPTV media functions realize a flexible and hierarchical media delivery architecture for effective delivery of contents in a distributed environment.

The main tasks of MCFs are summarized as follows:

- Mapping of content ID and content location to the corresponding MDF and selection of relevant MDFs.
- Management the content storage, propagation of content to distribution networks and control of the content distribution to media delivery functions and user equipment.
- Interaction with the UE (e.g., handling of video-recorder-like RTSP commands), control of network personal video recorder (PVR) and network time-shift TV.
- Collection of statistical information about service usages.

The MDFs are responsible for delivery of media to the user equipment (in IPTV domain, media may be video, voice as well as data). They have following main tasks:

- Storage of media (e.g., Content on Demand 'CoD' assets) and service information.
- Handling media flow delivery, content protection (e.g., content encryption) and Encoding (or transcoding) media to various media formats (e.g., various TV resolutions, depending on terminal capabilities or user preferences).

3.1.2 IPTV Non IMS architecture

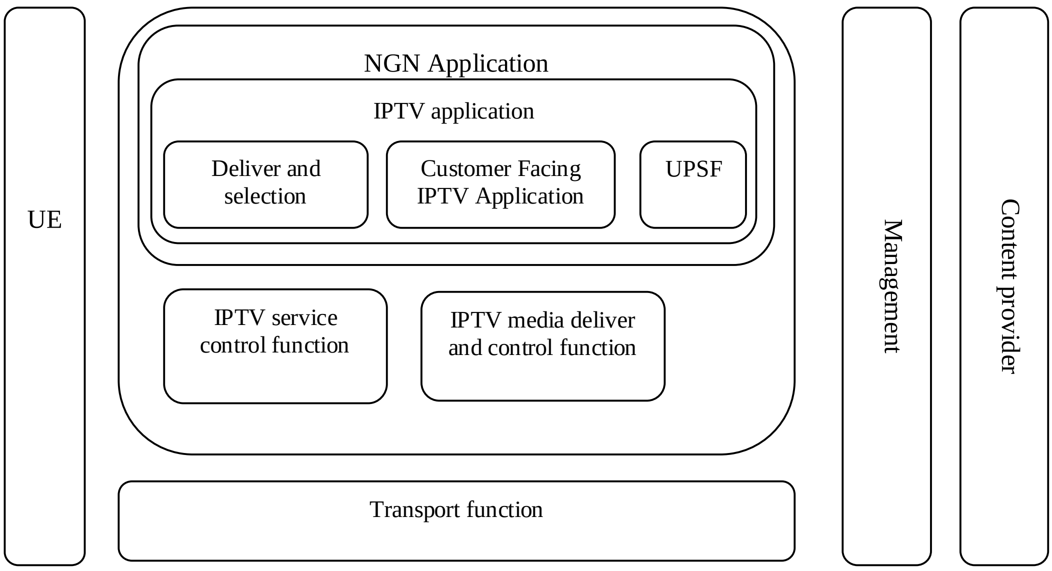


Figure 3-3: NGN IPTV Functional Architecture [ETSI TS 182 028]

The NGN-IMS-based IPTV architecture uses Core IMS Functions to provide service control functions as well as the users' authentication. However the NGN non-IMS-based IPTV architecture uses other two entities Customer Facing IPTV Application (CFIA) and IPTV Service Control Functions (IPTV-C) to replace the Core IMS. Other entities like the Service Discovery and Selection Functions and the Media Control & Delivery Functions perform the same roles with the ones that are located in IMS based IPTV architecture. These two entities are specific in the Non-IMS IPTV architecture and the communications between the entities are based on the HTTP protocol.

Customer Facing IPTV Application (CFIA) provides IPTV service provisioning, selection and authorization. The main tasks of CFIA are summarized as follows:

- Provides to the UE initial entry point to the service navigation and selection.

- Verify user’s access right according to the IPTV user profile and provides authentication and authorization to validate the user's right based on the user profile.
- Authorizes the UE to access the IPTV Service Control and Delivery Functions.

The IPTV service control (IPTV-C) functions are responsible for the execution of a given instance of an IPTV service during the service consumption and for the selection of Media Control & Delivery Function. The IPTV-C is able to initiate resource reservation process for network resources needed by the IPTV service according to the capabilities of the UE.

3.2 Proposed Context-Aware System (CAS)

Through context-awareness, IPTV systems will no longer require the users to give explicit instructions at every step during their interaction with the system. Figure 3-4 presents the general architecture of the proposed context-aware system, which is a hybrid architecture including centralized and distributed entities. The centralized entity is mainly the Context-Aware Server (CAS) which is considered as an application server (AS), while other entities are distributed in the user sphere, the network, and the service platform as explained below.

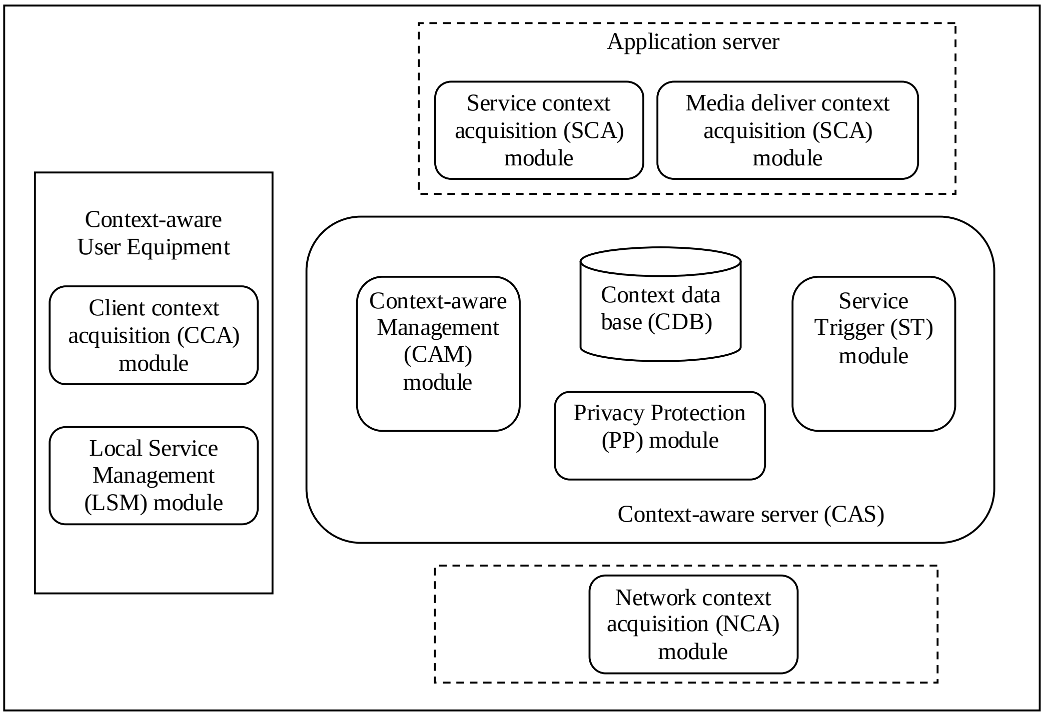


Figure 3-4 Proposed Context-aware system

3.2.1 Context-aware Server

The CAS includes four modules:

1) The Context-Aware Management (CAM) module: gathers the context information from the user, the application server and the network. CAM supports the context inference which helps in transforming lower level context information to a higher level context. The reasoning techniques such as rule based reasoning, probabilistic reasoning, etc could be used here.
2) The Context Database (CDB) module: stores the gathered and inferred context information and provides query interface to the Service Trigger (ST) module.
3) The Service Trigger (ST) module: has two functionalities, personalization of the established services according to the different context information, and discovering and setting up a personalized service for users according to the different contexts. The ST module communicates dynamically with the CDB module to monitor the context information before triggering the services, and communicates with the Privacy Protection (PP) module to verify if the services can use the context information or there are privacy constraints.
4) The Privacy Protection (PP) module: controls what data might be published, through verifying if the "ready to activate" services are authorized to access the required user context information or a part of it considering different privacy levels.

3.2.2 Context-aware User Equipment

The Context-aware User Equipment in the user domain includes two main modules:

1) The Client Context Acquisition (CCA) module discovers the context sources in the local sphere and collects the raw context information about user, device and environment. Sensors are the frequently used context sources which can be present in the user sphere, in the environment or in the device and retrieve context information from them. Different context information can be derived from these sensors, such as noises, lighting, proximity, user’s location, etc. These sensors detect the values and report this value to the CCA which then represents the received information in the predefined XML format and forwards it to the CAM module located in the CAS.

2) The Local Service Management module controls and manages the local services execution though monitoring the CCA module and dynamically comparing the context with its stored rules in order to activate the corresponding service in a personalized manner.

3.2.3 Service domain context-aware modules

There are two modules located in the service domain:

1) Service Context Acquisition (SCA) module collects the service context information and sends it to the CAM. Most service related context information is contained in the Electronic Program Guide (EPG). The SCA collects the EGP from the IPTV application or from the internet, and retrieves the information about title of the channel, description, starting time, ending time and other information like categories. SCA then represents the information in a XML format and forwards it to the CAM.
2) Media Delivery Context Acquisition (MDCA) module monitors the content delivery and dynamically acquires the network context information during the content delivery and sends it to the CAM. This information reflects the state of the network such as packet loss, jitter, and round-trip delay.

3.2.4 Network domain context-aware modules

In the network domain, a Network Context Acquisition (NCA) module is responsible for collecting the bandwidth information. In the NGN network, through consulting the Resource and Admission Control Sub-System (RACS) before each service session establishment, and sending the acquired information to the CAM.

3.3 Context-aware IPTV/IMS solution

3.3.1 Architecture

An extension to the IPTV/IMS architecture is proposed through integrating the proposed context-aware system described in the previous section. Figure 3-5 illustrates the new architecture. This architecture benefits from the HSS to store the static user context information including: user's personal information (age, gender …), subscribed services and preferences. The SCA module is integrated in the IPTV Service Selection functional (SSF) module and acquires the service context information making use of the Electronic Program Guide (EPG) received by the SSF from the content provider, and which includes content and media description. The MDCA module is integrated in the Media Function (MF) to dynamically acquire the network media information, where the MF employs the Real Time Transport Control Protocol (RTCP) to control the content delivery through dynamically gathering network information statistics (mainly information on the packet loss, jitter, and round-trip delay reflecting the network context) for a media session. On the other hand, the NCA module is integrated in the classical RACS to collect the initial network context information (mainly bandwidth). Finally, the CCA and LSM modules represent an extension on the UE (User Equipment) to collect the different user and device contexts in the user domain.

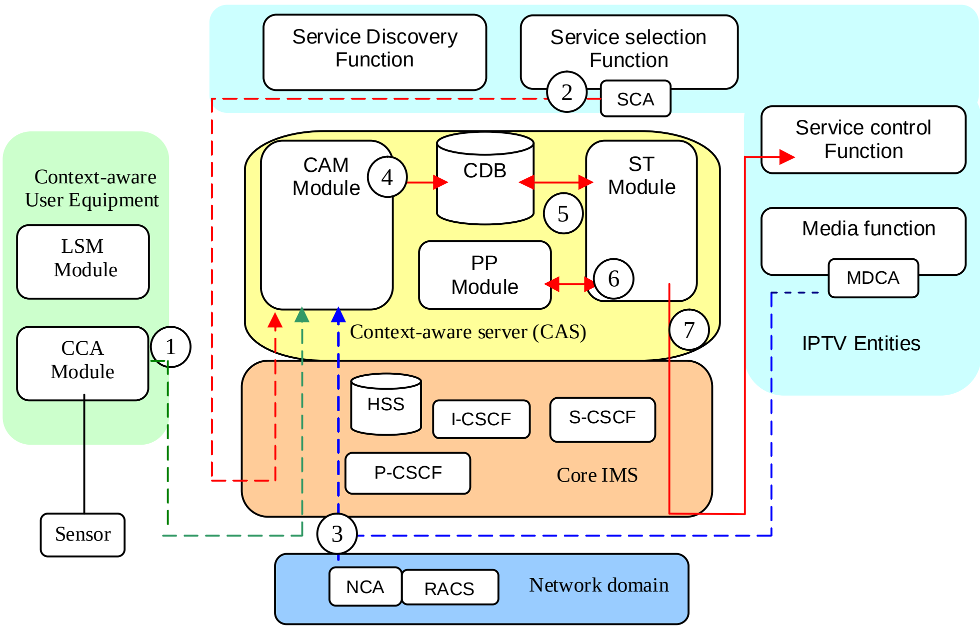


Figure 3-5 Proposed context-aware IPTV/IMS architecture

In order to provide the personalized TV Service, the CCA, SCA, NCA and MDCA modules respectively gather the user/device context information, service context information and network context information and send them to the CAM (steps 1-3). After each acquisition of the different context information, the CAM in the CAS analyzes the collected information and derives higher level context information which is stored in the CDB (step 4). The ST module continuously communicates with the CDB module to monitor the context information, according to which the ST can discover the need for personalizing the established services or setting up a new service (step 5). Before triggering the service it communicates with the Privacy Protection (PP) module to verify if the corresponding service can use the existing context information (step 6). If there is no privacy constraint, the ST module sends to the Service Control Function (SCF) a message for triggering the service, encapsulating the needed context information in this message (step 7). Then, this latter activates the service according to the received context information. The communication between the ST module and the SCF replaces the classical process in classical IPTV/IMS service access, where the user directly communicates with the SCF for requesting the service.

3.3.2 Context information gathering and transmission

Context gathering determines how the context information could be collected from the distributed sources to the application. It is very important to the context-aware service especially for the client-server model, where the transfer of context information needs to take place over unreliable and dynamically changing networks. The efficiency of the context gathering is a critical factor for the performance of the whole context-aware system. The SIP protocol is chosen as the context gathering and transmission transport protocol for the IMS based context-aware IPTV architecture. Because the SIP protocol is chosen as the signaling protocol for the IMS based application and used for controlling communication sessions for the IMS based IPTV service. This solution benefits from the existing interfaces for the context distribution (interfaces between UE, SSF, MF and IMS). Another reason is that SIP is a text-based protocol which contains a message body and very suitable for the context transmission. The context information is contained in the message body of different SIP methods (like SUBSCRIBE, PUBLISH, NOTIFY). The XML document is chosen because it can be well integrated into the SIP message. The following subsection explains the context gathering and transmission in the proposed context-aware IPTV architecture.

The communication between the different architectural entities takes place through the contextual service registration and the context information transmission between the end-user/network/application servers and the CAS.

Contextual Service Registration: This procedure extends the classical IMS user registration and authentication procedure to include users' static context information acquisition from the HSS. The Diameter Server-Assignment-Answer message [3GPP TS 29.229] which is sent by the HSS to the S-CSCF in the classical IMS registration is extended to include the user static context information by adding a User-Static-Context Attribute Value Pair. The Context-Aware REGISTER (CA-REGISTER) message is defined extending the SIP protocol

REGISTER message [Rosenberg 02], which enables context-awareness and transmits the user static context information, delivered at the S-CSCF from HSS, to the CAS.

User/Device Dynamic Context Information Transmission: This procedure is newly proposed to allow the CCA module of the UE to update in the CAS the user/device context information that it dynamically acquires. The Context-PUBLISH message is defined, extending the classical SIP PUBLISH message in order to publish the context information. The representation of the context information in the Context-PUBLISH message follows the predefined XML format, while the context information attributes representing the user and device context (mainly concerning user's location (indoor location), devices location, supported network type, supported media format, and screen size) as illustrated in the Figure 3-6. The CAS replies by a CA-OK (Context-awareness OK) message, which is similar to the SIP OK message. Figure 3-7 illustrates the Context-PUBLISH message.


```
PUBLISH sip:user_public@home.net SIP/2.0
Max-Forwards: 70
Via:    SIP/2.0/UDP [5555::1:2:3:4]
Route: <sip:pcscf@home.net: >, <sip:scscf@home.net;>
From: <sip:user1_public@home.net>;tag=31415
To: <sip:user_public@home.net>
Call-ID: b89rjhnedlrfjflslj40a222
CSeq: 61 PUBLISH
Event: CONTEXT
Expires: 7200
Content-Type: application/pidf+xml
Content-Length: (...)
<?xml version="1.0" encoding="UTF-8"?>
 <context xmlns="urn:ietf:params:xml:ns:pidf"
              xmlns:dm="urn:ietf:params:xml:ns:pidf:data-model"
              xmlns:rpid="urn:ietf:params:xml:ns:pidf:rpid"
              entity="pres:user_public@home.net">
   <dm:person id="1234">
      <rpid:place-type><rpid:home/></rpid:place-type>
      <rpid:location><rpid:salon/></rpid:location>
      <rpid:network-type><rpid: ADSL/></rpid: network-type>
   </dm:person>
   <dm:device id="1">
      <rpid:location><rpid:salon/></rpid:location>
      <rpid:suppported_network_type> <rpid:fix><rpid:suppported_network_type>
      <rpid:supported_media_format><rpid:mpeg2/><rpid:supported_media_format>
      <rpid:screen_size><><rpid:screen_size>
    </dm: device>
 </context>
```


Figure 3-6 User context information

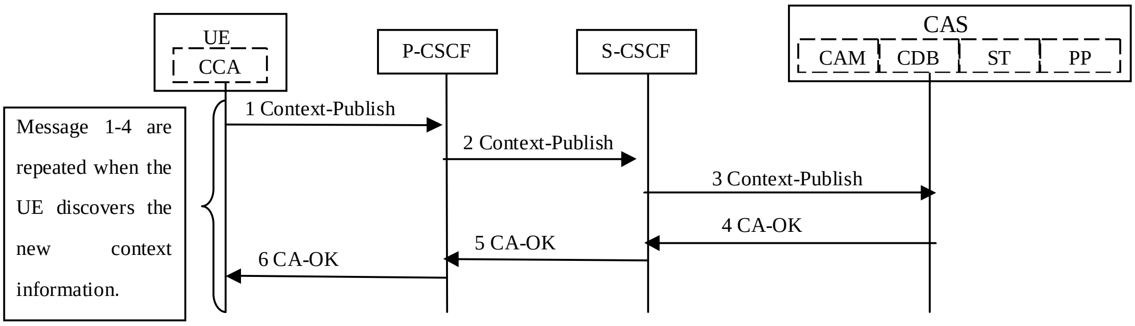


Figure 3-7 Context-Publish message for the User context transmission

Service context Information Dynamic Transmission: This procedure is similar to the procedure of the user context information dynamic transmission to the CAS allowing the dynamic update for service information acquired by the SCA module through extracting the service context information from the Electronic Program Guide (EPG) received by the SSF. The Context-PUBLISH message illustrated in Figure 3-8 is used to transfer the service context information from the SCA in the SSF to the CAS via the S-CSCF. The representation of the context information in the Context-PUBLISH message follows the predefined XML format, while the context information attributes representing the service context (mainly, the service start-time, end-time, content-type and codec). The CAS replies by a CA-OK (Context-awareness OK) message, which is similar to the SIP OK message.

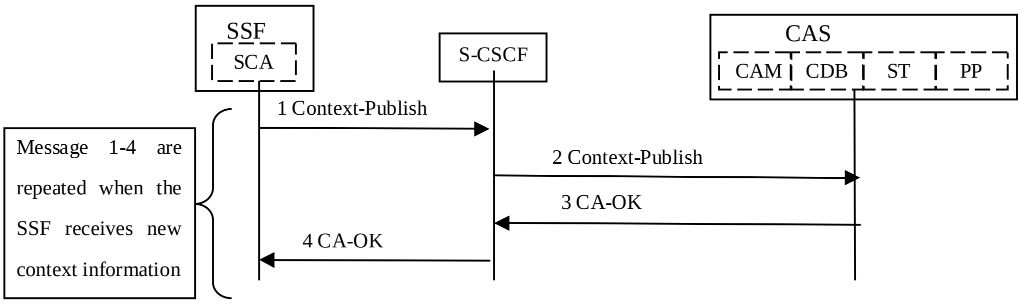


Figure 3-8 Context-Publish message for the service context transmission

Network Context Information Transmission during the Session Initiation: This procedure concerns the network context information transmission during the session initiation through extending the classical resource reservation process. In this latter, the P-CSCF receiving the service request sends a Diameter protocol AA-Request message to the Resource and Admission Control Sub-System (RACS) for the resource reservation. Based on the available resources, the RACS will decide whether to do or not a resource reservation for the service. An AA-answer message is sent by the RACS to the P-CSCF for informing the latter the results of the resource reservation (successful resource reservation or not). This process is extended in order to send the bandwidth information to the P-CSCF, where the NCA module integrated in the RACS in the extended architecture generates a Context AA-Answer message extending the AA-Answer message through adding a Network-Information Attribute Value Pair to include the bandwidth information. The P-CSCF in turn sends this information to the CAS via the S-CSCF through a Context-Publish message. Figure 3-9 illustrates this process.

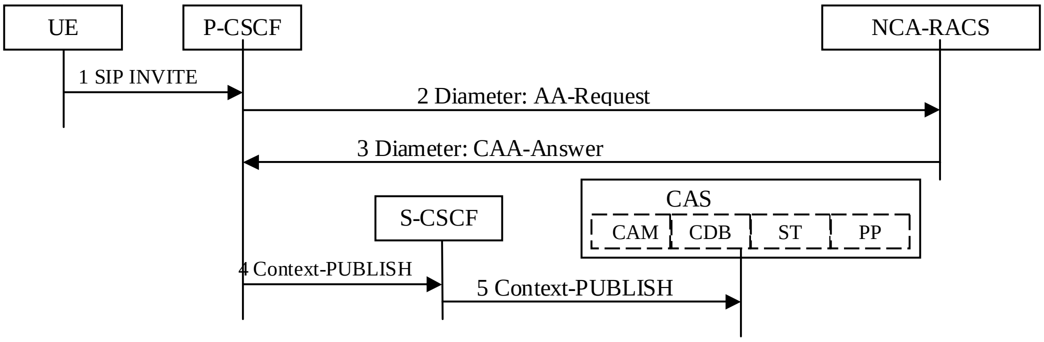


Figure 3-9 Context-Publish message for the network context transmission

Network Context Information Dynamic Transmission: This procedure allows the MDCA module to dynamically transmit the network context information related to the media session to the CAS. The Context-PUBLISH message illustrated in Figure 3-10 is used, where the representation of the network context information follows the XML format including context information attributes representing the network context (mainly, jitter, packet loss and delay). The extraction of the network context information, related to the media session by the MDCA, makes use of the existing RTP (Real-time Transport Protocol)/ RTCP [Schulzrinne 03] reports/statistics during the media session. The Context-PUBLISH message is used to transfer the context information by the MDCA module to the CAS via the P-CSCF and S-CSCF.

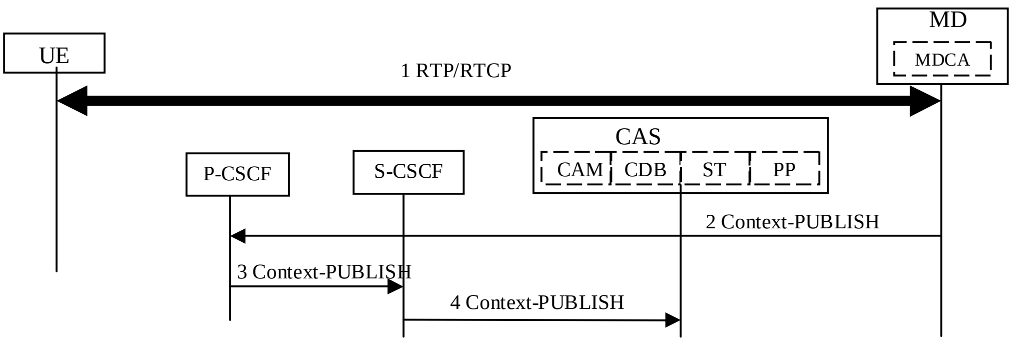
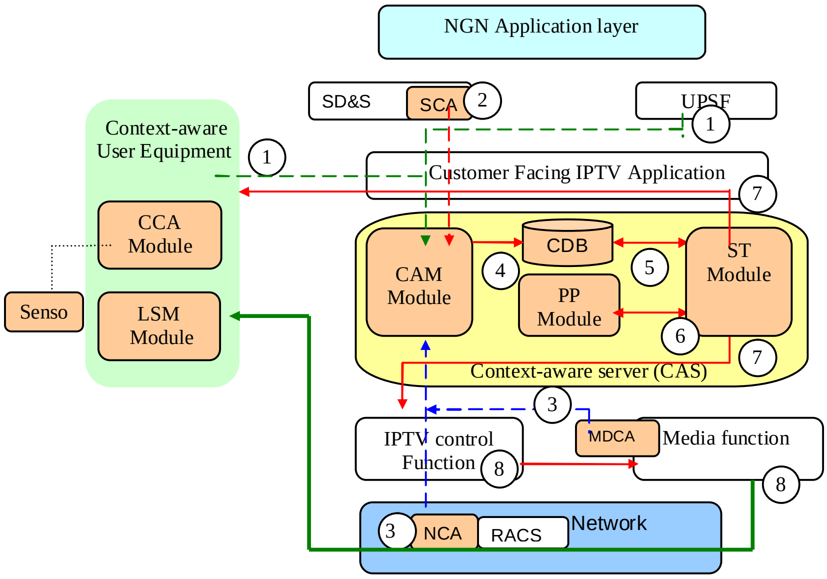


Figure 3-10 Context-Publish message for the dynamic network context transmission

3.4 Context-aware IPTV/non-IMS solution

3.4.1 Architecture

A solution is proposed for context-aware IPTV/non-IMS services, aiming to widen the scope of the contribution and to minimize the dependence on IMS. Figure 3-11 presents the proposed IPTV/Non-IMS architecture integrating the proposed context-aware system for IPTV service personalization.



1. User and device context information and transmission
2. Service context information and transmission
3. Network context information and transmission
4. Context information storage in the CDB.
5. ST communication with the CDB for monitoring context information and services discovery.
6. ST communicates with the PP for privacy constraints verification.
7. ST requests to trigger the personalized services.
8. Adapted content to the UE

Figure 3-11 Proposed context-aware IPTV/Non-IMS architecture

This architecture benefits from the User Profile Service Function (UPSF) to store the static user context information including: user's personal information (age, gender, …), subscribed services and preferences. The SCA (Service Context Acquisition) is integrated in the SD&S IPTV functional module and acquires the service context information making use of the EPG (Electronic Program Guide) received by the SD&S from the content provider, and which includes content and media description. The MDCA (Media Delivery Context Acquisition) is integrated in the MF to dynamically acquire the network media information, where the MF employs the Real Time Transport Control Protocol (RTCP) to control the content delivery through dynamically gathering network information statistics (mainly information on the packet loss, jitter, and round-trip delay which reflects the network context) for a media session. On the other hand, the NCA (Network Context Acquisition) module is integrated in the classical RACS (Resource and Admission Control Sub-System) to collect the initial network context information (mainly bandwidth). Finally, the CCA (Client Context Acquisition) and LSM (Local Service Management) modules represent an extension on the UE (User Equipment).

After each acquisition of the different context information (related to the user, devices, network and service), the CAM (Context-Aware Management) in the CAS (Context-Aware Server) infers the collected information and derives higher level context information which is stored in the CDB (Context Data Base). The ST (Service Trigger) module continuously communicates with the CDB module to monitor the context information, according to which the ST can discover the need for personalizing the established services or setting up a new services. To do so, the ST module gets the stored context-information from the CDB and uses it while triggering the corresponding service. Before triggering the service it communicates with the PP (Privacy Protection) module to verify if the corresponding service can fully use the existing context information. If there is no privacy constraint, the ST module activates the personalized services.

3.4.2 Context information gathering and transmission

The architecture benefits from the existing interfaces (interface between UE and CFIA, interface between SSF and CFIA, interface between CFIA and IPTV-C) to transfer the context information. New interfaces are also defined between CFIA, IPTV-C and MF to communicate with the CAS to transfer the context information. The protocol used on these new defined interfaces is HTTP. HTTP is chosen as the context transmission protocol as the HTTP protocol is chosen in IPTV non-IMS case in the communication process. Another reason is that HTTP is also a text-based protocol which could easily contain more context information in the body message. The previously defined XML file can also be used in the HTTP protocol. Furthermore HTTP is used in non-management TV (as WEB TV) which is promising for interoperation of the work.

The communications procedures for the context gathering and transmission is differs from the IMS Core in the following: 1) the transport protocol used for the Non-IMS context-aware IPTV architecture is HTTP; and 2) the context information is directly transferred from the context source to the IPTV system without a control layer (Core IMS as in the IMS based IPTV architecture). The details of the context gathering and transmission are as follows:

Contextual Service Registration: This procedure extends the classical IPTV service initiation and authentication procedure to include user's static context information acquisition. The user's static context information is stored in the UPSF. We extend the Diameter Server-

Assignment-Answer message which is sent by the UPSF to the CFIA to include the user static context information by adding a User-Static-Context Attribute Value Pair (AVP). We use the HTTP POST message to transmit the user static context information, stored in the UPSF, to the CAS.

User/Device Dynamic Context Information Transmission: This procedure is proposed to allow the CCA module of the UE to update in the CAS the user/device context information that it dynamically acquires. We use the HTTP POST message to transmit the context information. The representation of the context information in the HTTP POST message follows the predefined XML format, while the context information attributes representing the user and device context (mainly concerning user's location (indoor location), devices location, supported network type, supported media format, screen size, and the network type) as illustrated in the Figure 3-12. The CAS replies by a HTTP OK message. Figure 3-13 illustrates the User/Device Dynamic Context Information Transmission

```
POST /users HTTP/1.1
Host: CAS
Content-Type: application/xml
Content-Length: (...)
<?xml version="1.0" encoding="UTF-8"?>
 <context xmlns="urn:ietf:params:xml:ns:pidf"
          xmlns:dm="urn:ietf:params:xml:ns:pidf:data-model"
          xmlns:rpid="urn:ietf:params:xml:ns:pidf:rpid"
          entity="pres:user_public@home.net">
   <dm:person id="1234">
     <rpid:place-type><rpid:home/></rpid:place-type>
     <rpid:location><rpid:salon/></rpid:location>
     <rpid:network-type><rpid: ADSL/></rpid: network-type>
   </dm:person>
   <dm:device id="1">
     <rpid:location><rpid:salon/></rpid:location>
     <rpid:suppported_network_type> <rpid:fix><rpid:suppported_network_type>
     <rpid:supported_media_format><rpid:mpeg2/><rpid:supported_media_format>
     <rpid:screen_size><><rpid:screen_size>
    </dm: device>
 </context>
```

Figure 3-12 User context information

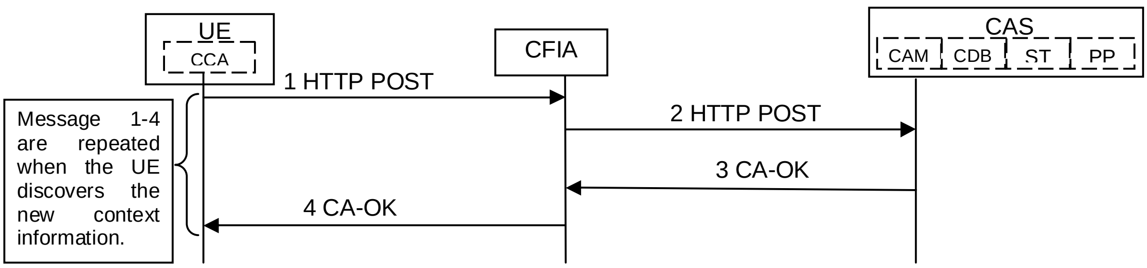


Figure 3-13 User/Device Dynamic Context Information Transmission

Service context Information Dynamic Transmission: This procedure is similar to the procedure of the user context information dynamic transmission to the CAS and the dynamic update for service information, where the HTTP POST message is also used. The service information is acquired by the SCA module through extracting the service context information from the Electronic Program Guide (EPG) received by the SSF, and transferred to the CAS via CFIA. The representation of the context information in the HTTP POST message follows the predefined XML format, while the context information attributes representing the service context (mainly, the service start-time, end-time, content-type and codec). Figure 3-14 illustrates the HTTP POST message which includes the attributes representing the service context.

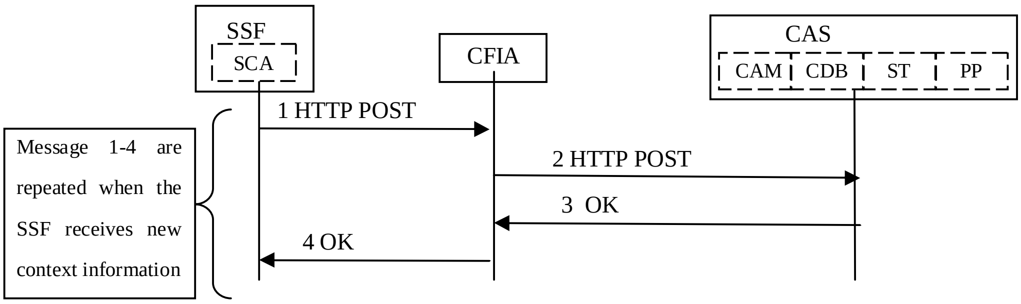


Figure 3-14 Context-Publish message for the service context transmission

Network Context Information Transmission during the Session Initiation: This procedure concerns the network context information transmission during the session initiation through extending the classical resource reservation process. In this latter, the IPTV-C receiving the service request sends a Diameter protocol AA-Request message to the Resource and Admission Control Sub-System (RACS) for the resource reservation. Based on the available resources, the RACS will decide whether to do or not a resource reservation for the service. An AA-answer message is sent by the RACS to the IPTV-C for informing the latter the results of the resource reservation (successful resource reservation or not). We extend this process in order to send the bandwidth information to the IPTV-C, where the NCA that we proposed to integrate in the RACS generates a Context AA-Answer (CAA-Answer) message extending the AA-Answer message through adding a Network-Information Attribute Value Pair to include the bandwidth information. Figure 3-15 illustrates the HTTP POST message which includes the attributes representing the network context.

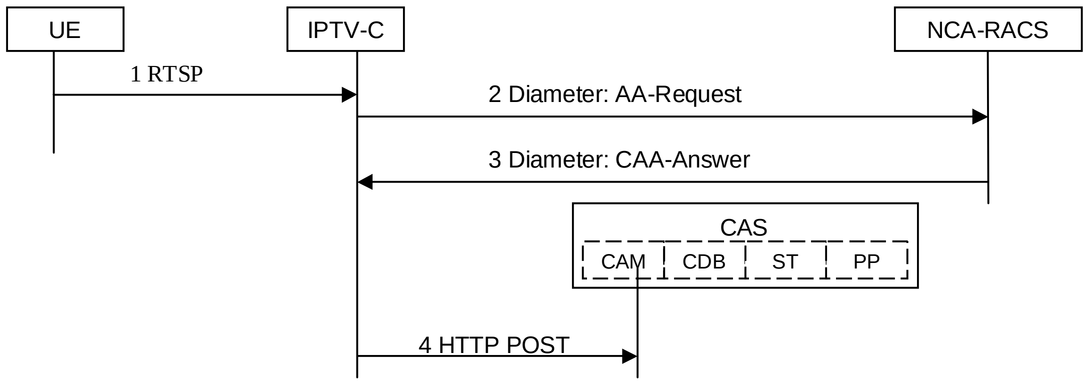


Figure 3-15 Context-Publish message for the network context transmission

Network Context Information Dynamic Transmission: This procedure allows the MDCA to dynamically transmit the network context information related to the media session to the CAS. The HTTP POST message is used, where the representation of the network context information follows the XML format including context information attributes representing the network context (mainly, jitter, packet loss and delay). As illustrated in Figure 3-16, the HTTP POST message is used to transfer the context information by the MDCA module to the CAS via the CFIA.

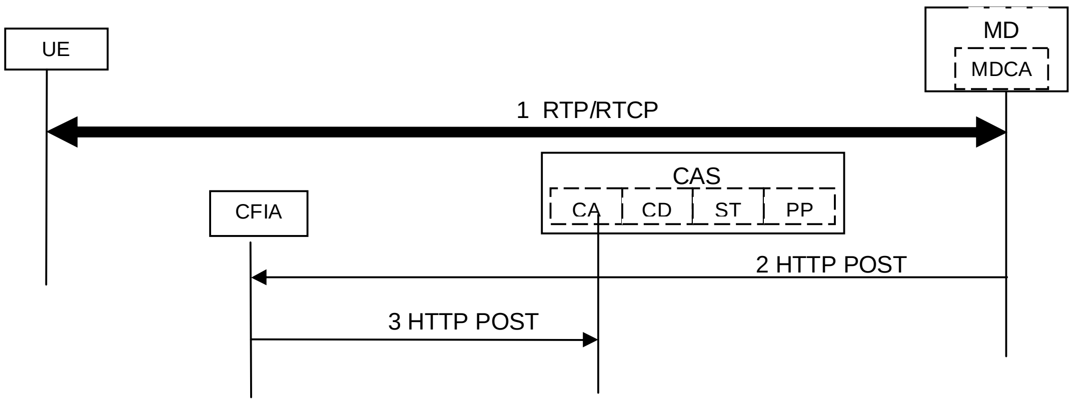


Figure 3-16 Context-Publish message for the dynamic network context transmission

3.5 Implementation and Performance Analysis

3.5.1 Overview on implementation

An implementation is carried out for the personalized IPTV system (the context-awareness system, the personal identification and content personalization mechanisms) and the implemented modules are integrated on top of NGN IPTV architecture. A proof of concept is achieved through the correct functioning of the proposed system and a performance evaluation through several performance metrics is done. This implementation is integrated in the platform of European project "UP-TU-US" (".User-Centric Personalized IPTV UbiquitOus and SecUre Services ") managed by Orange Labs

Figure 3-17 illustrates the architecture of the platform. The context-aware server (CAS) is developed using the framework Ruby on Rail [Ruby] which is a high level framework for the HTTP services development and implemented on a machine with Intel Xeon E3110 3.00Ghz, 1GB RAM. The implemented CAS is integrated to an NGN IPTV architecture implemented on 5 machines for respectively the IPTV-C, CFIA, SD&SF, MF IPTV functional entities and the UPSF. The Service Context Acquisition (SCA) module is implemented in the SD&SF to collect the service context information from the EPG. At the end-user side, the STB is implemented on a PC machine which contains three functional modules: traditional STB module (dealing with the authentication, session negotiation and service reception, etc.), the Client Context Acquisition (CCA) and Local Service Management (LSM) modules of the context-aware system. A VLC library is used in the STB to process the IPTV streams coming from the Media Function.

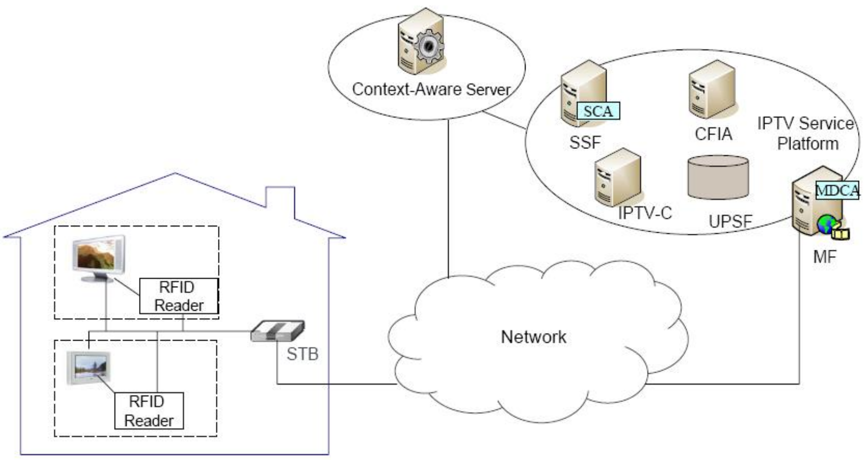


Figure 3-17 Implementation platform architecture

In order to collect user dynamic context information and identify the different users, the RFID technology [Landt 01] is employed allowing each user to use an RFID tag to identify himself to the system. In addition, each user device (for example TV or PC Screen) is connected to an RFID reader indicating the identity of the device which is associated to the device location. When the user comes next to the device, the RFID reader of this device reads the user's identity and sends it to the STB together with the device identity in the reader. The STB could then know the user location through the reference to the location of the device that is being used by the user. The STB sends the user and device context information to the CAS. Then the ST in the CAS sends the personalized EPG to the user function of the acquired context information and the LSM in the STB select the content the best matches the acquired context information.

3.5.2 System evaluation and performance analysis

The platform with the implemented modules was firstly tested from the functional point of view and observing the right functioning of the whole system with TV Live and VoD (Video on Demand) IPTV services. Then a performance evaluation of the proposed solution for TV Live and VoD IPTV services is done and compared with the traditional IPTV case without personalization.

3.5.2.1 Performance metrics used

This subsection defines the metrics used in the performance analysis.

1) Delay of personalized content selection (DPS): defined as the consumed time from sending the first context update request from user until receiving the personalized EPG from the CAS. This delay includes the new context information transmission, treatment and the personalized EPG generation. The DPS reflects the performance of the CAS. Since there could be large number of users request the personalized content at the same time, the increase of the DPS with the increase of the end users is analyzed.

2) Delay of the service initiation (DSI): defined as the consumed time from the start of the STB to the reception of the IPTV service (when the video starts playing). In traditional IPTV case, this delay includes the delay of user's authentication, session negotiation and video display. In the proposed solution, besides the mentioned delay, DSI also includes the delay of personalized content selection (DPS).

3) EPG Browsing Time (EBT): measures the user's quality of experience (QoE) level in terms of how quickly a user can find his preferred program from the displayed EPG. EBT presents the consumed time from the display of the EPG until finding the user's preferred content.

To derive the EBT for the traditional EPG browsing, it is considered that there are n programs on the EPG and that the probability of the preferred program (i) selection by the user is the same for all the programs (probability = 1/n). It is also assumed that during the EPG browsing, the user will watch the selected program for a duration (t') before switching to another program. So the expected traditional EBT can be calculated as:

$$E(EBT) = \sum_{i=1}^{n} \frac{1}{n}(i-1)\, t' = \frac{n-1}{2} t' \qquad (1)$$

Another important parameter "accuracy probability Pa" is introduced, reflecting how well the personalized EPG programs meet the user's expectation.

From the definition of the accuracy probability, the matching of the EPG programs to the user's expectation has the following probabilities: the first program matching probability is (Pa); the second program matching probability is (1-Pa)Pa and the mth program matching probability is (1-Pa)m-1Pa. So the expected browsing time for our solution can be calculated as:

$$E(EBT) = \sum_{i=1}^{n} (1-p_a)^{(i-1)} p_a (i-1)\, t' = \left((1-p_a)\frac{1-(1-p_a)^{n-1}}{p_a} + (1-n)(1-p_a)^n \right) t' \qquad (3)$$

3.5.2.2 Performance analysis

From the Figure 3-18, an increase is observed in the delay of personalized content selection (DPS) when the number of end users increases. However the increase rate is small and slows down with the increase of users. When the number of user increases from the 50 to 400, the increase rate of the DPS is about 3%, and when the number of user increase from 400 to 1000, the increase rate of the DPS is about 0.5%. This shows the scalability of the proposed solution with the increase in the number of users.

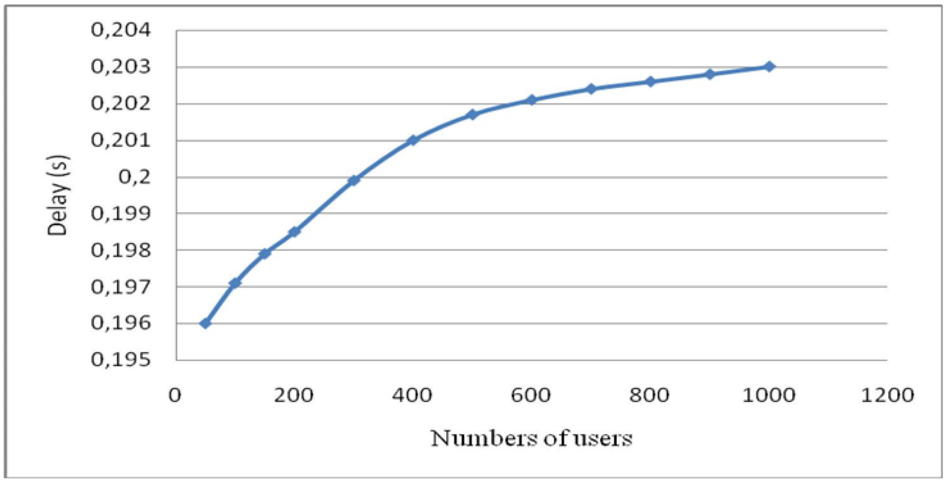


Figure 3-18 Delay of the personalized content selection

Figure 3-19 presents the delay of the service initiation for both traditional IPTV and personalized IPTV cases. For traditional IPTV case, a delay of 1.75 and 2.12 seconds is observed respectively for the initiation of TV Live and VoD services. While, for the personalized IPTV case, a delay of 2.04 and 2.29 seconds is observed respectively for the initiation of TV Live and VoD services presenting a slight increase of about 0.20 seconds compared to the traditional IPTV case. This increase is mainly due to the consumed time for context information acquisition, treatment and personalization and service selection. Although not all the functions in the actual IPTV platform are considered, compared with the average delay of service initiation which is about 2.9 seconds [Cruz 09], the proposed solution does not impact the performance of the service.

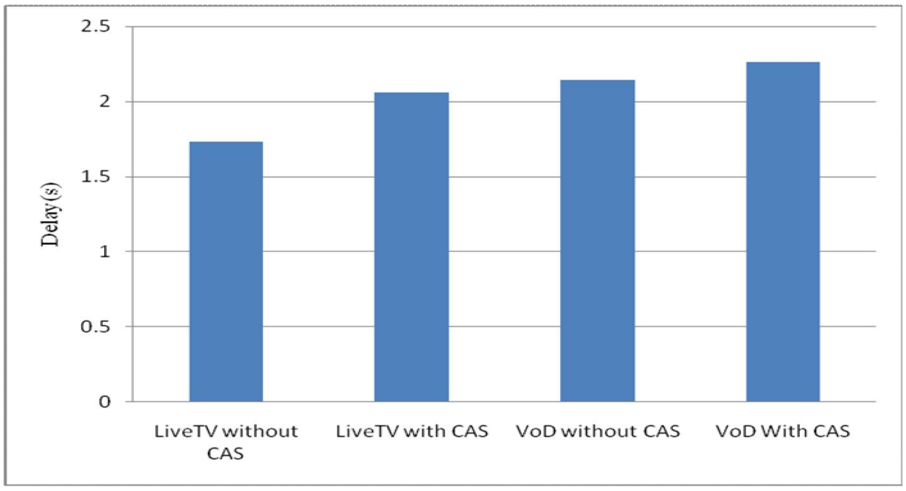


Figure 3-19 Delay of service initiation

Figure 3-20 illustrates the obtained values for the EBT in the presence of various numbers of programs for the TV Live service. In the traditional IPTV case, the EBT linearly increases with the increase in the number of programs indicating poor QoE with the explosion of the number of programs. To calculate the EBT for the proposed solution, the EPG accuracy probability (Pa) is firstly measured through verifying the matching of the received personalized EPG to the users in the case of different users with different context information changes. Among several services requests, the Pa was found to be 0.8 (i.e. about 80% of the recommended contents correspond to users' interest). By substituting this obtained Pa value in equation (3) together with the change of the value of (n) reflecting the number of programs, the EBT values illustrated in Figure 3-20 are obtained for the personalized TV case. A slight increase is observed at first with the increase in the number of programs then a constant EBT value is shown in spite of the number of programs, thus confirming the gain in terms of QoE with our proposed solution with the increase in the number of programs.

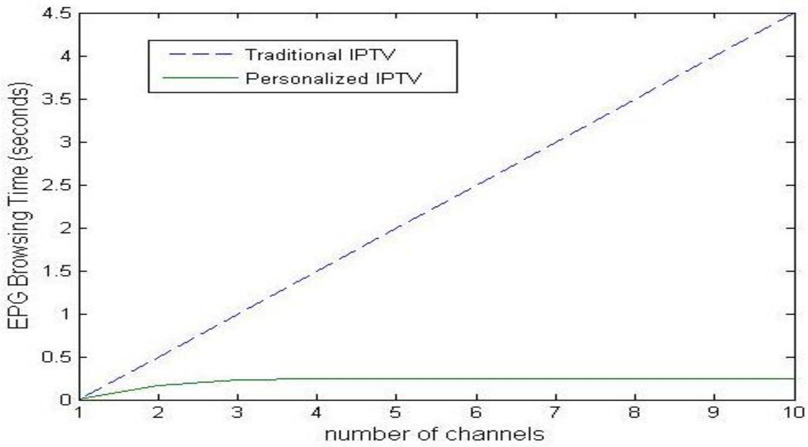


Figure 3-20 EPG Browsing time

3.6 Conclusion

IPTV market evolution is a promising technology allowing satisfying users' experience and presenting advanced entertainment services and business opportunities for network operators, service providers and content providers. In such TV model, context-awareness is promising in monitoring users' environment (including networks and terminals), interpreting users' requirements and making users' interaction with the TV dynamic and transparent. However, a problem that is not yet resolved is how to achieve TV services personalization using technologies like context-awareness on top of NGN IPTV architecture in a standard manner.

This chapter proposes a context-aware system for IPTV and integrates it into the IPTV/IMS architecture and IPTV/Non-IMS architecture to allow IPTV service personalization in a standard manner. These new context-aware IPTV architectures allow the user to participate in his profile construction by giving/collecting his context information in a dynamic manner. It is expected to enhance the different offers of services provided by network operators and opens new business opportunities for network operators and many more actors (content providers, service providers, equipments manufactures …) in the multimedia domain. Since the proposed context-aware system is not fully centralized and users' identities are not attached to the used devices, the proposed solution could assure personalized IPTV services access during mobility within the domestic sphere and could assure nomadic access of personalized IPTV service.

The proposed solution is easy to deploy as it extends the existing IPTV/IMS architecture and IPTV/Non-IMS architecture (standardized at the ETSI/TISPAN) and existing protocols (standardized within the IETF). Furthermore, service acceptability by users could be easily assured thanks to the privacy consideration through a special privacy management entity. The proposed solution is implemented on top of an IPTV platform validating its correct functioning and evaluating its performance for TV Live and VoD IPTV service compared to classical IPTV case (with no personalization). Interesting results are obtained for the proposed solutions in terms of the personalized content selection and service initiation delays as well as the EPG browsing time, which proves the success of the proposed system.

Part II Personalized Users' Access

Chapter 4 Personalized Identification & Authentication

To provide personalized IPTV service, the system needs to aware of which user is watching the TV. Identifying each user enables IPTV system to know "who is watching TV" and to personalize the content accordingly. Indeed, user's identity is a part of the user context. User's identification and authentication solutions need to be applied to current IPTV system in order to indentify each user and personalize his access. Authentication and information protection observe lot of attention in NGN, where users' authentication to the IMS takes place through the AKA (Authentication and Key Agreement) protocol, while Generic Bootstrapping Architecture (GBA) is used to authenticate users before accessing the multimedia services over HTTP. However, the tight attachment of the subscriber authentication to the user equipment limits the personalization of the services and does not allow unique identification for each user if several users share the same equipment. To solve this problem, a new identification and authentication mechanism using RFID and the Identity Based cryptography (IBC) is proposed in this chapter. This solution employs a personal identity for each user during services authentication aiming to enhance services personalization and to allow new social services since it employs a personal identity for each user (which could be mapped to his presence).

4.1 Identification & authentication in NGN: General overview and related work

In NGN, IMS (IP Multimedia Subsystem) secures the service access through authentication and providing session keys for the integrity protection. A major component to secure the IMS is the ISIM (IMS SIM) card [Priselac 08]. Each subscriber uses an ISIM card holding a stored secret key, shared between the user and the Home Subscriber Server (HSS) in the operator Home network, to be able to authenticate to the IMS network and to access the IMS services. The authentication to IMS services is based on the Session Initiation Protocol (SIP) and is directly coupled to the user registration process, where the authentication is carried out based on the Authentication and Key Agreement (AKA) protocol [RFC 3310]. Besides SIP-based services, several services are accessed over HTTP. In order to allow the access to HTTP-based services in a secure manner, IMS uses the Generic Bootstrapping Architecture (GBA)

[3GPP TS 133.220], which also employs the AKA protocol. Indeed, the AKA protocol creates a tight attachment to the user equipment, where each user should have his own devices (with his own ISIM cards) in order to be correctly identified and authenticated to his own services. This fact limits the personalized access of each user and hence limits the service personalization. The strong dependency on the ISIM card stands as an obstacle towards compatibility with different services belonging to different service providers and also limits the security performance [Priselac 08]. In addition, using AKA in IMS proved to have some weakness, like short key for cryptographic purposes [3GPP2S]. The solution in [Wu 09] proposed to strengthen IMS security through defining a new AKA protocol based on Elliptic Curve Cryptography (ECC) which has some advantages like smaller key sizes, faster computations, more efficient data transmission. In [Huang 07], a new AKA protocol called one pass AKA is also proposed for UMTS networks. This solution has one round-trip capacity to realize the mutual authentication and key agreement and reduces 50% of the message delivery cost compared with the traditional IMS AKA authentication. In [Ring 06] a new AKA mechanism for SIP was designed using Identity Based Cryptography (IBC) in which the public key can be derived from public information that uniquely identifies the user [Boneh 01]. However, in these solutions, the user's identity is always the tight attached to the user equipment that limits the personalization of the services.

4.2 Users Identification and authentication in NGN

4.2.1 Users identification

In IMS, each user has two types of identities: IP Multimedia Private Identity (IMPI) and IP Multimedia Public Identity (IMPU). IMS user shall have one or more IMPIs (to be used with different user's devices), but there is only one private identity stored in each ISIM card having the form of a Network Access Identifier (NAI: The standard syntax is "user@realm"). The home network operator assigns the private identity for being used in registration, authentication, authorization, administration, and accounting purposes. The IMS user shall have one or more IMPUs and each ISIM card stores at least one public identity. The public identities are used by any user for requesting communications to other users and to services access. The IP Multimedia Public Identity takes the form of a SIP Universal Resource Identifier (URI) or the "tel:"-URI format.

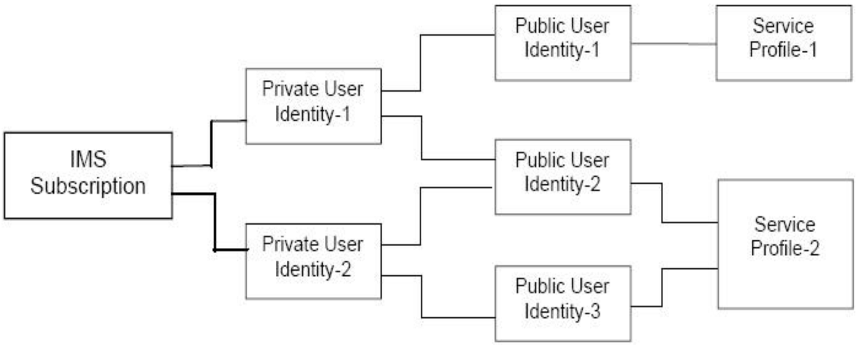


Figure 4-1. Relationship between IMS Identities (source [3GPP TS 123 228])

Figure 4-1 shows the relationship between the IMPI, the IMPU and the services. This figure presents the Service Profile as a collection of services, where user related data are stored in the HSS (Home Subscriber Subsystem). Each IMPUs is associated to one and only one service profile; however each service profile can be associated to one or more IMPU. Different IMPIs can share the same IMPU within the same IMS subscription. Hence, an IMPU can be simultaneously registered from multiple User Equipments (UEs) that can use different IMPIs and different contact addresses.

4.2.2 IMS Authentication during Users' Registration

Authentication and key agreement in IMS is known as IMS AKA, which is based on a secret shared key *sk*, shared between the user (ISIM card) and the HSS (Home Subscriber Server). This authentication in IMS is directly coupled to the SIP registration process. The HSS never directly communicates with the User Equipment (UE), it is the Serving Call Session Control Function (S-CSCF) in IMS that performs the authentication process.

Figure 4-2 shows the steps for user's authentication with the IMS core network.

- In order to be authenticated, the UE sends the IMPU stored in the ISIM card in the initial REGISTER request (message 1).
- Upon the reception of the REGISTER request, the P-CSCF examines the "home domain name" to discover the I-CSCF (message 2).
- Then, this latter sends a query to the HSS to find the appropriate S-CSCF, and then forwards the REGISTER request to the S-CSCF (messages 3-5).
- When receiving this REGISTER request, the S-CSCF downloads an array of n (n>=1) AVs (Authentication Vector) from the HSS (messages 6-7). The AVs are ordered based

on sequence numbers (SQN) and each AV includes a random challenge (RAND), the expected result (XRES), the network authentication token (AUTN), an Integrity Key (IK) and a Ciphering Key (CK).

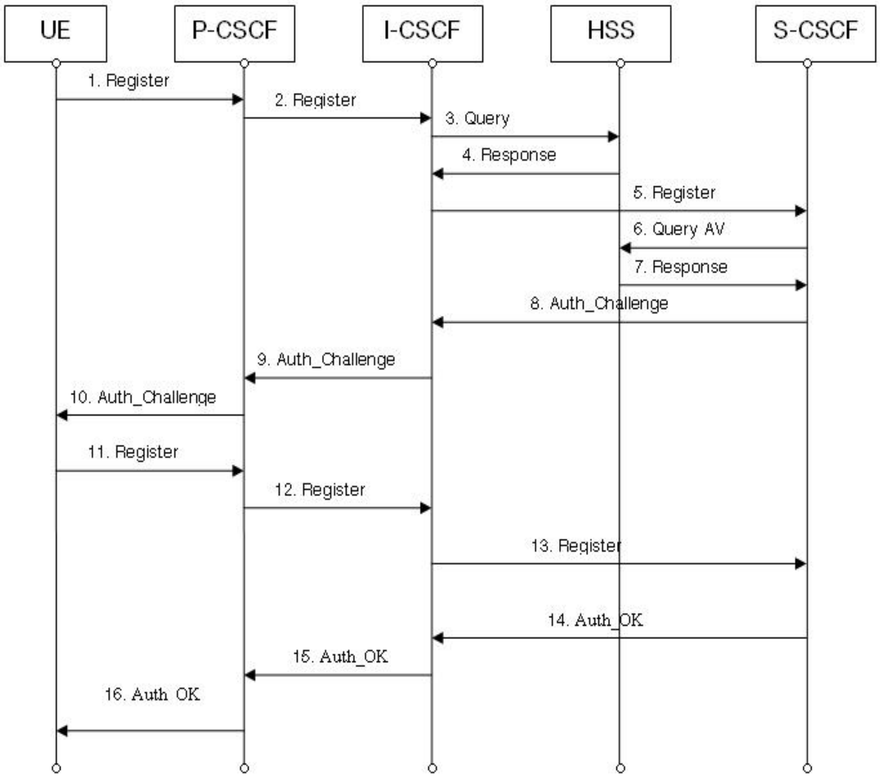


Figure. 4-2 Authentication to the IMS during Users' Registration

- Then the S-CSCF sends to the user through the P-CSCF an authentication request within a "401 (Unauthorized) response", which includes: the RAND, the AUTN, the IK and the CK (message 8-9).
- The P-CSCF, when receiving the "401 Unauthorized response", removes the IK and CK from the response before relaying it to the UE (message 10).
- Upon receiving the unauthorized response, the UE extracts the MAC (Message Authentication Code) and the SQN from the AUTN. It also calculates the XMAC (expected message authentication code) and checks if the XMAC matches the received MAC and if the SQN is in the correct range. If both checks are successful the network is authenticated. Then the UE calculates the challenge response RES and sends it to the S-CSCF (messages 11-13).

- The UE also calculates the resulting IK which is then shared between the P-CSCF and the UE as the base of the Security Association. When the S-CSCF receives the response, it compares the RES and XRES that were received in the AV from the HSS. The UE authentication process will end up as successful with either a "SIP OK" message or a "SIP unauthorized message", both message are sent by the S-CSCF to the UE (message 14-16).

4.2.3 Generic Bootstrapping Architecture and HTTP based Services Authentication

Generic Bootstrapping Architecture (GBA) was designed by the third Generation Partnership Project (3GPP) to authenticate each user before accessing the multimedia services over HTTP using the HTTP Digest AKA protocol. There are four entities constituting the GBA: User Equipment (UE), Network Application Function (NAF), Bootstrapping Server Function (BSF) and Home Subscriber Server (HSS).

1) User Equipment (UE): contains parameters for identifying the user and Authentication & Key Agreement information for the HTTP Digest AKA protocol applied in the authentication.

2) Home Subscriber Server (HSS): stores the GBA user security settings (GUSSs) for the GBA authentication applying HTTP Digest AKA protocol. The GUSS contains the list of the user's identities required for the applications and also the authorization information.

3) Bootstrapping Server Function (BSF): is a central entity in the GBA. The BSF and the UE mutually authenticate using the AKA protocol, and agree on the session keys that are applied afterwards between the UE and the Network Application Function.

4) Network Application Function (NAF): communicates securely with the BSF with which the user is connected to acquire a shared key material established between the UE and the BSF. It can authorize the user to certain applications based on the authorization information in the GUSS.

Figure 4-3 gives the procedure of the GBA authentication applying HTTP-Digest approach.

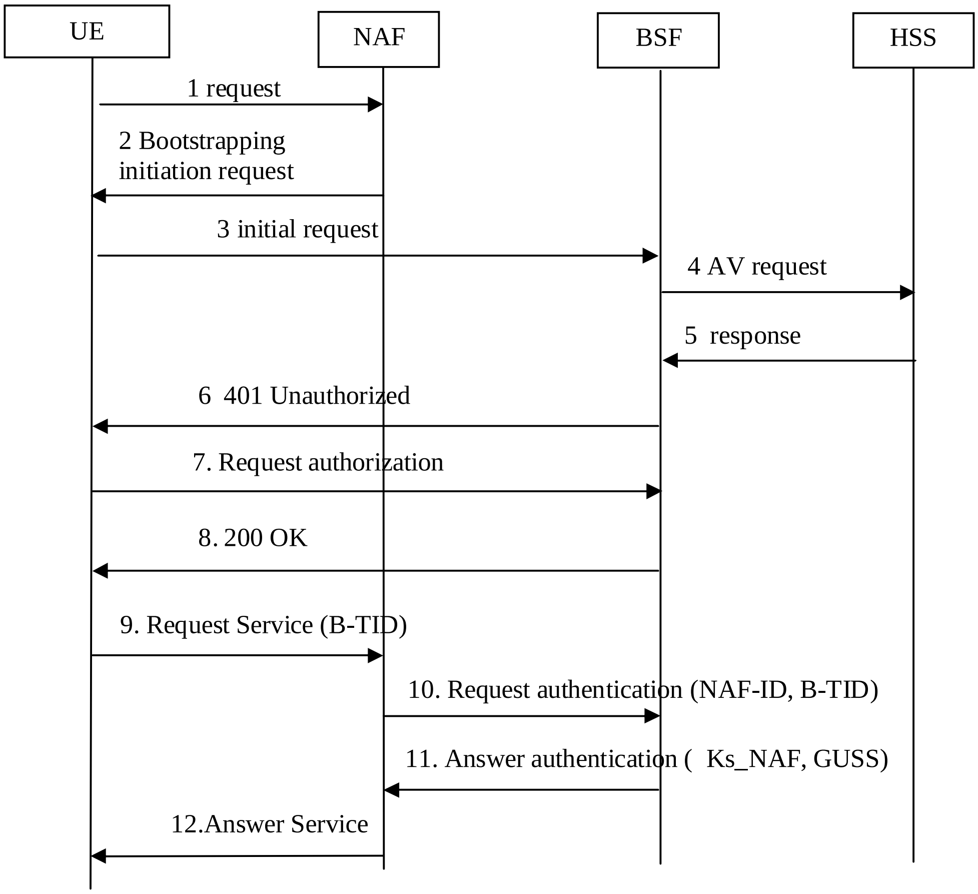


Figure 4-3 GBA authentications for services access in IMS

- To grant service access to the UE, the latter communicates with the NAF to verify if the bootstrapping procedure is needed (message 1).
- If it is the case and if there are no available bootstrapping parameters in the UE (message 2), the UE will send an HTTP GET request including the user private identity (IMPI) to the BSF to initiate the bootstrapping procedure (message 3).
- The BSF then requests from the HSS an array of n (n>=1) authentication vectors (AVs) and the GBA User Security Settings (GUSS) corresponding to the IMPI (messages 4-5).
- AVs are ordered based on sequence numbers (SQN) and each AV includes a random challenge (RAND), the expected result (XRES), a network authentication token (AUTN), an Integrity Key (IK) and a Ciphering Key (CK). In order to authenticate the

UE, the BSF forwards the RAND and AUTN to the UE in a “401 (Unauthorized) message” without the CK, IK and XRES (message 6).

- Upon receiving the unauthorized response, the UE extracts the MAC (Message Authentication Code) and the SQN from the AUTN. It also calculates the XMAC (expected message authentication code) and checks if the XMAC matches the received MAC and if the SQN is in the correct range. If both checks are successful the network is authenticated. Then the UE calculates the authentication challenge response RES and also computes the IK and CK. The UE sends another HTTP request to the BSF, containing the Digest AKA response which is calculated using RES (message 7).
- The BSF authenticates the UE by verifying if the expected response matches the received challenge response. If the check is successful then the user has been authenticated and the user private identity IMPI is registered in the BSF. The BSF generates key material Ks by concatenating CK and IK. The BSF also generates the bootstrapping transaction identifier (B-TID) for the IMPI and sends a 200 OK message, including the B-TID, to the UE to indicate the success of the authentication (message 8).
- The UE also calculates the key material Ks using CK and IK. Both the UE and BSF use the Ks to derive the NAF specific key (Ks-NAF). The UE contacts the NAF and provides the B-TID and a digest calculated using Ks-NAF (message 9).
- The NAF then requests the corresponding Ks-NAF and GUSS from the BSF by sending the B-TID (message 10).
- After receiving the BSF response (message 11), the NAF calculates the corresponding digest values using Ks-NAF obtained from the BSF, and compares the calculated value with the received value from the UE. If the verification succeeds, the NAF sends 200 OK response to the UE to indicate the success of the authentication (message 12). The NAF can also use Ks-NAF for integrity protection and to authenticate the response.

4.3 SA-IBC (Service Authentication based on Identity Based Cryptography) Solution

This section presents a new authentication solution named SA-IBC (Service Authentication based on IBC) which employs RFID on one hand to identify each user and employs the Identity Based Cryptography (IBC) on the other hand to generate the private keys of the UE instead of using AKA mechanisms during the GBA authentication for HTTP-based services. This approach allows service personalization through identifying and authenticating users in a personal manner during services access and is suitable to IPTV services personalization.

4.3.1 RFID based identification

The main limitation in IMS identification is the attachment of the user's identity to the user equipment, where each user should have his own devices (with his own ISIM cards) in order to be correctly identified and authenticated to his own services. This fact limits the personalized access of each user and hence limits the service personalization.

There are several user identification solutions aiming to offer personalized access. The frequently used solution is login and password. However asking users to enter their login and password on a keyboard every time they turn on the TV is not very user-friendly and is not likely to be successful. SA-IBC uses the RFID (Radio Frequency Identification) for identification solution because of its capability to distinguish each user, low cost and the fact that it can be easily integrated in the current IPTV STB.

RFID uses radio waves to transfer data between a reader and a tag that contains the item data. Every RFID tag consists of two parts: an antenna and an integrated circuit. The role of the antenna is sending and receiving a radio-frequency signal used to communicate with an RFID reader. The role of the integrated circuit is modulating and de-modulating this signal as well as storing and processing information. When the tag receives a signal sent out by an RFID reader, this circuit modulates the incoming signal with some information stored inside the tag (usually a serial number). The modulated signal is then sent back to the reader by the antenna. Finally, the reader receives the signal and performs de-modulation to extract the information.

The RFID reader is connected to other applications which perform other activities based on the information collected by the RFID reader from the tags. RFID can be used for a wide variety of applications, ranging from user identification to public transportation tickets and from supply chain labels to building access control. Consequently, SA-IBC employs RFID for personalized identification of users during IPTV services access.

4.3.2 Identity Based Cryptography

The Identity Based Cryptography (IBC) is a cryptosystem in which a public key for the user is generated using the identity of the user (e.g. a user's email address) [Shamir 84]. It has a trusted central authority named Private Key Generator (PKG) that uses a master secret to generate private keys for users. Each user should authenticate himself to the PKG to obtain the private key to be used to decrypt the cipher messages that he receives, and that are encrypted with the public key of the user. Figure 4-4 illustrates the different functions in IBC. When a user (Alice) wishes to send an encrypted message to another user (Bob), she first generates Bob's public key KpubBob based on a public identity for Bob. Then, she encrypts the message M with KpubBob and sends this encrypted message C to Bob. When Bob receives the message, he needs to decrypt it. He authenticates himself to the PKG to obtain the secret key KprivBob to decrypt the cipher message C and obtains the plaintext message M.

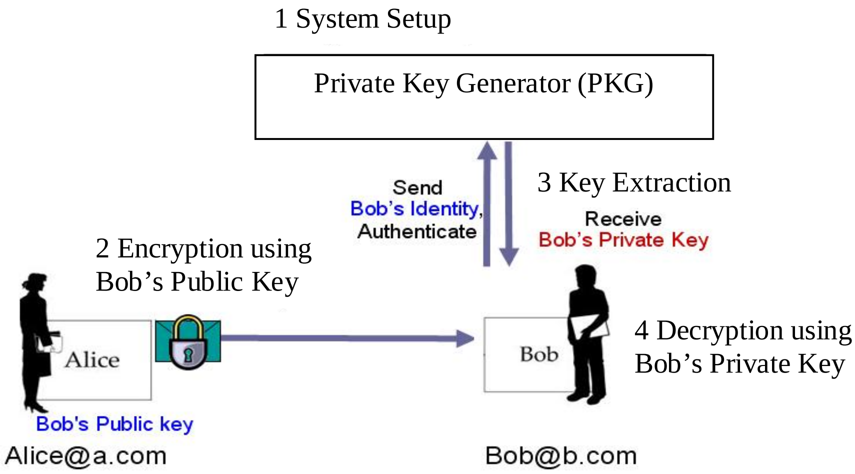


Figure. 4-4 Functions in IBC

4.3.3 SA-IBC Solution Description

This solution requires the integration the of the RFID reader into the UE, where each user needs to employ the RFID tag to identify himself to the system. The user's identity UserID and password are stored on his RFID tag. When the tag is read out by an RFID reader, the user's identity and password are transferred from the RFID tag to the terminal. The terminal then initiates the SA-authentication, which consists of a Bootstrapping phase using the BSF and a secure communication phase between the UE and the NAF. A service authentication based on GBA architecture is considered and hence the PKG is integrated within the Home Subscriber Server (HSS) without modifying the traditional HSS function. Figure 4-5 illustrates SA-IBC and the following steps explain its different functions:

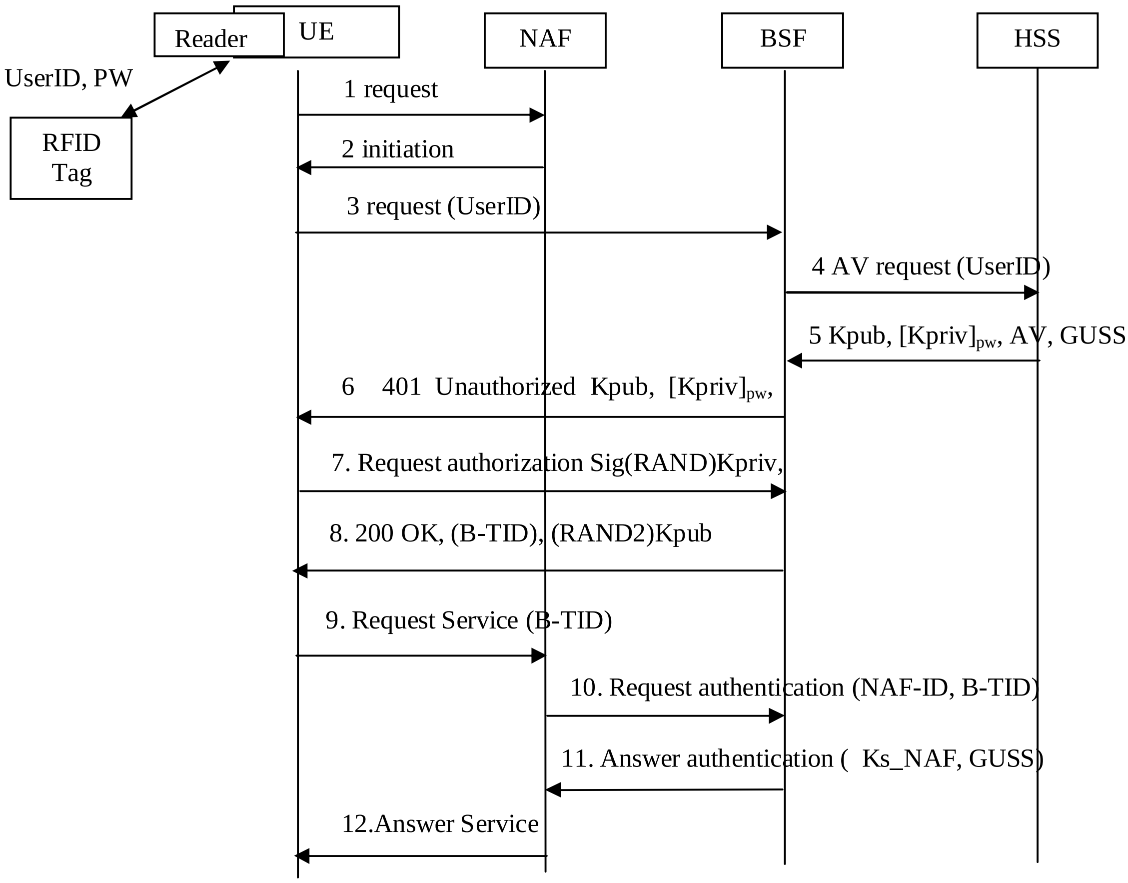


Figure 4-5 SA-IBC Authentication solution

- Firstly, the user uses his RFID tag to identify himself to the system. The RFID tag sends the stored user identity (UserID) and password (pw) to the RFID reader, which is connected to the UE. Then the UE communicates with the NAF to verify if the bootstrapping procedure is needed (message 1). The UserID is contained in this message.
- If there are no available bootstrapping parameters for the user (message 2), the UE will contact the BSF by sending an HTTP request including the user identity UserID (message 3).
- The BSF communicates with the HSS to request Authentication Vector (AV) and GBA User Security Settings (GUSS). According to the UserID, the HSS finds out user's password. The PKG in HSS uses the UserID to generate the user's public key (Kpub)

and private key (Kpriv) and encrypts UE's private key using user's password. The HSS sends Kpub, encrypted Kpriv, the Authentication Vector (containing RAND and PKG parameters) and the GUSS to the BSF (messages 4-5).

- Then the BSF forwards the AV (RAND and PKG parameters), the public key Kpub and the encrypted Kpriv to the UE in the 401 (Unauthorized) message. (message 6).
- After receiving the message from the BSF, the UE extracts its private key Kpriv using the user's password. Then, it generates a signature of the RAND value using Kpriv through Elliptic Curve Digital Signature Algorithm (ECDSA) [X9.62]. The PKG parameters, Kpub, Kpriv are used as the inputs to the ECDSA Algorithm. The UE sends the signature of the RAND to the BSF in an HTTP request in order to authenticate itself (message 7).
- The BSF verifies the signature using Kpub. After the successful verification, the BSF generates the B-TID, and chooses another random value 'RAND2' to generate Ks_NAF = KDF (RAND2, Kpub). KDF is the key derivation function used in the tradition GBA authentication [3GPP TS 133.220]. The BSF encrypts the 'RAND2' using Kpub and sends the encrypted [RAND2]Kpub and B-TID to the UE in 200 OK message (message 8).
- When UE receives the message from the BSF, he decrypts the [RAND2]Kpub using Kpriv and generates the Ks_NAF= KDF (RAND2, Kpub). Then the UE sends an HTTP message to the NAF to request service. In the message, the UE supplies the B-TID to the NAF to allow the NAF to retrieve the corresponding ks_NAF from the BSF (message 9).
- The NAF sends an HTTP message to the BSF which includes B-TID received in message 9 and the NAF-ID for GUSS (message 10).
- The BSF replies to the NAF with the key Ks_NAF and the GUSS. Ks_NAF is the session key between UE and is used for securing the communication between them (message 11). Then the NAF starts the service with UE (message 12).

4.4 Implementation and performance analysis

4.4.1 Implementation Environment

The GBA architectural entities, precisely the servers NAF, BSF and HSS are emulated using C++. Each emulated server runs on a dedicated machine with Intel® Core ™2 CPU @ 1,80GHz 1 GB RAM. Eight clients (UEs) are setup on eight different PCs with the same capacity. Each UE is considered as a client of both the BSF and the NAF; the NAF is considered as a client of the BSF; and the BSF plays the role of a server for the NAF and the UE. Figure 4-6, gives an overview of the implemented architecture.

HTTP has been implemented through the SOCKET to realize the communication between the servers and the clients. In order to allow the servers and the clients to easily generate HTTP messages and to extract the information from the received HTTP messages, two parsers are developed using LEX [Levine 92]. To realize the encryption/decryption functions and the private/public key pair generation function, the Miracl library [Miracl] is used.

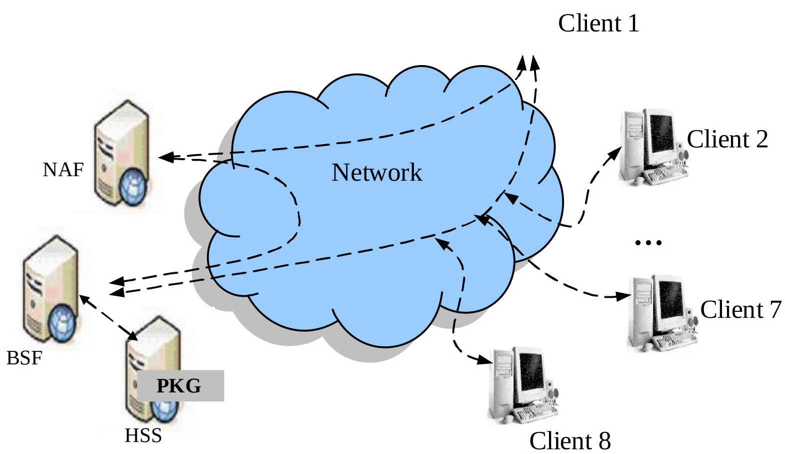


Figure 4-6 Overview of the implemented architecture

4.4.2 Performance metrics

To carry out the implementation tests for SA-IBC, the test scenario considers 2n (n=0, 1, 2, 3, 4) clients starting the authentication request at the same time and defining 3 values for the authentication failure probability: PAF = 0 (no failure), PAF = 0.25 (25% of the clients fail to be authenticated) and PAF = 0.5 (50% of the clients fail to be authenticated).

The following performance metrics are used to evaluate the SA-IBC performance: i) authentication request processing time on each server and ii) resources consumed during the service authentication phase.

A) Authentication request processing time on Servers

The authentication request processing time is defined as the time spent to treat the authentication request on the NAF and the BSF, including message parsing, message encryption/decryption, and key generation times. In the case of authentication failure, the authentication process stops at message 8 of SA-IBC in figure 4-5, and hence the processing time on the NAF and the BSF is reduced. Ts_{NAF} and Ts_{NAF}' are used to represent the processing time on the NAF respectively in the case of authentication success and failure. So, the expectation value of the authentication request processing time on the NAF is calculated as follows:

$$E(Ts_{NAF}) = Ts_{NAF}(1 - P_{AF}) + \left(Ts'_{NAF} P_{AF} + Ts_{NAF} P_{AF}(1 - P_{AF})\right) + \left(Ts'_{NAF} P_{AF}^2 + Ts_{NAF} P_{AF}^2 (1 - P_{AF})\right) + Ts'_{NAF} P_{AF}^3 \quad (1)$$

$Ts_{NAF}(1- P_{AF})$: represents the authentication request processing time on the NAF in the case of a client receiving the authentication success message after the first authentication attempt.

$(Ts_{NAF}'P_{AF} + Ts_{NAF}P_{AF}(1-P_{AF}))$: represents the authentication request processing time on the NAF in the case of a client receiving the authentication success message after the second authentication attempt.

$(Ts_{NAF}'P_{AF}^2 + Ts_{NAF}P_{AF}^2(1-P_{AF}))$: represents the authentication request processing time on the NAF in the case of a client receiving the authentication success message after the third authentication attempt.

$Ts_{NAF}'P_{AF}^3$: represents the authentication request processing time on the NAF in the case of a client receiving authentication failure messages after the three authentication attempts.

Similar to (1), the expectation value of the authentication processing time on the BSF is calculated as follows:

$$E(Ts_{BSF}) = Ts_{BSF}(1 - P_{AF}) + \left(Ts'_{BSF} P_{AF} + Ts_{BSF} P_{AF}(1 - P_{AF})\right) + \left(Ts'_{BSF} P_{AF}^2 + Ts_{BSF} P_{AF}^2 (1 - P_{AF})\right) + Ts'_{BSF} P_{AF}^3 \quad (2)$$

$Ts_{BSF}(1 - P_{AF})$: represents the authentication request processing time on the BSF in the case of a client receiving the authentication success message after the first authentication attempt.

($Ts_{BSF}'P_{AF} + Ts_{BSF}P_{AF}(1-P_{AF})$): represents the authentication request processing time on the BSF in the case of a client receiving the authentication success message after the second authentication attempt.

($Ts_{BSF}'P_{AF}^2 + Ts_{BSF}P_{AF}^2(1-P_{AF})$): represents the authentication request processing time on the BSF in the case of a client receiving the authentication success message after the third authentication attempt.

$Ts_{BSF}'P_{AF}^3$: represents the authentication request processing time on the BSF in the case of a client receiving authentication failure messages after the three authentication attempts.

B) Resources consumption during authentication

The authentication consumed resources S_{NAF} and S_{BSF} are respectively defined as the consumed resources in terms of memory on the NAF and BSF during each service authentication operation. If there are multiple authentication requests that arrive at the servers (NAF and BSF) at the same time, the average consumed resources is considered.

The consumed resources for an authentication request are considered similar in the cases of both authentication success and failure since resources are allocated when the servers receive the authentication request. Then the expectation value of the authentication consumed resources on the NAF and BSF is calculated as follows:

Consumed resources on the NAF

$$\begin{aligned} E(S_{NAF}) = S_{NAF}(1-P_{AF}) + (S_{NAF}P_{AF} + S_{NAF}P_{AF}(1-P_{AF})) + \\ (S_{NAF}P_{AF}^2 + S_{NAF}P_{AF}^2(1-P_{AF})) + S_{NAF}P_{AF}^3 \end{aligned} \tag{3}$$

$S_{NAF}(1-P_{AF})$: represents the authentication consumed resources on the NAF in the case of a client receiving the authentication success message after the first authentication attempt.

($S_{NAF}P_{AF} + S_{NAF}P_{AF}(1-P_{AF})$): represents the authentication consumed resources on the NAF in the case of a client receiving the authentication success message after the second authentication attempt.

($S_{NAF}P_{AF}^2 + S_{NAF}P_{AF}^2(1-P_{AF})$): represents authentication consumed resources on the NAF in the case of a client receiving the authentication success message after the third authentication attempt.

$S_{NAF}P_{AF}^3$: represents the authentication consumed resources on the NAF in the case of a client receiving authentication failure messages after the three authentication attempts.

Consumed Resources on the BSF:

$$E(S_{BSF}) = S_{BSF}(1-P_{AF}) + (S_{BSF}P_{AF} + S_{BSF}P_{AF}(1-P_{AF})) + \\ (S_{BSF}P_{AF}^2 + S_{BSF}P_{AF}^2(1-P_{AF})) + S_{BSF}P_{AF}^3 \qquad (4)$$

$S_{BSF}(1-P_{AF})$: represents the authentication consumed resources on the BSF in the case of a client receiving the authentication success message after the first authentication attempt.

$(S_{BSF}P_{AF} + S_{BSF}P_{AF}(1-P_{AF}))$: represents the authentication consumed resources on the BSF in the case of a client receiving the authentication success message after the second authentication attempt.

$(S_{BSF}P_{AF}^2 + S_{BSF}P_{AF}^2(1-PAF))$: represents authentication consumed resources on the BSF in the case of a client receiving the authentication success message after the third authentication attempt.

$S_{BSF}P_{AF}^3$: represents the authentication consumed resources on the BSF in the case of a client receiving authentication failure messages after the three authentication attempts

4.4.3 Experimental Results and Performance Analysis

This section presents the performance evaluation of the obtained results based on the defined performance metrics, while comparing the obtained values of those metrics with the derived ones.

The measured values of the different parameters in equations (1)-(4) are illustrated in Table 4-1.

Table 4-1 Obtained Experimental values for some parameters

Parameters Types	**Parameters Values**
Ts_{NAF}, Ts_{BSF}, Ts_{HSS} – Authentication Success Case	31ms, 50ms, 28ms
Ts_{NAF}', Ts_{BSF}', Ts_{HSS}' – Authentication Failure Case	4.5ms, 28ms, 28ms
NAF Consumed resources (S_{NAF})	48Kb
BSF Consumed resources (S_{BSF})	102Kb

These values are acquired from the log files generated in the clients and servers. These log files record the sent time and received time of each message and also the consumed resources in real-time.

Figure 4-7 illustrates the average authentication request processing time on the servers (NAF and BSF) among the 2n clients during the experimentation time. A nearly constant processing time is noticed although the increase in the number of clients, because the authentication request treatment for a client has no impact on the treatment for other clients. On the other hand, the processing time gets longer with the increase in the authentication failure probability due to numerous authentication attempts. The calculated authentication processing time in equations (1) and (2) are compared with the obtained authentication processing time through resolving equations (1) and (2) using the measured processing time parameters in Table 4-1. It is observed that the calculated values conform to the obtained ones in Figure 4-7. Some illustrative examples are: in the case of only 1 client and no authentication failure (p=0 a calculated TsNAF = 31 ms and TsBSF = 50 ms are obtained, in the case of 4 clients with 25% of authentication failure (P=0.25), a calculated TsNAF = 31,8 ms and TsBSF = 58,4 ms are obtained, in the case of 8 clients with 50% of authentication failure (P=0.5) a calculated TsNAF = 31 ms and TsBSF = 68,2 ms are obtained.

Figure 4-8 illustrates the average resources consumed for the authentication process on the NAF and BSF for the 2n clients during the whole experimentation time. A nearly constant value is observed although the increase in the number of clients. On the other hand, there is an increase in the consumed resources with the increase of the authentication failure probability due to the more authentication attempts. Furthermore, it is noticed that the BSF consumes more resources compared to the NAF due to the fact that BSF processes more HTTP messages and carries out more encryption/decryption calculation. Indeed, the BSF presents a bottleneck during the process of service authentication. To obtain better performance and scalability, BSF function needs to be distributed through including several BSF servers. The calculated consumed resources in equations (3) and (4) are compared with the obtained consumed resources through resolving equations (3) and (4) using the measured consumed resources parameters in Table 1. We observed that the calculated values conform to the obtained ones in Figure 4-8. Some examples are: in the case of only 1 client and no authentication failure (p=0) a calculated SNAF = 48 kb, and SBSF = 102 kb are obtained, in the case of 4 clients with 25% of authentication failure (P=0.25), a calculated SNAF = 63 kb and SBSF = 134 kb are obtained, in the case of 8 clients with 50% of authentication failure (P=0.5) a calculated SNAF = 84 kb and SBSF = 178 kb are obtained.

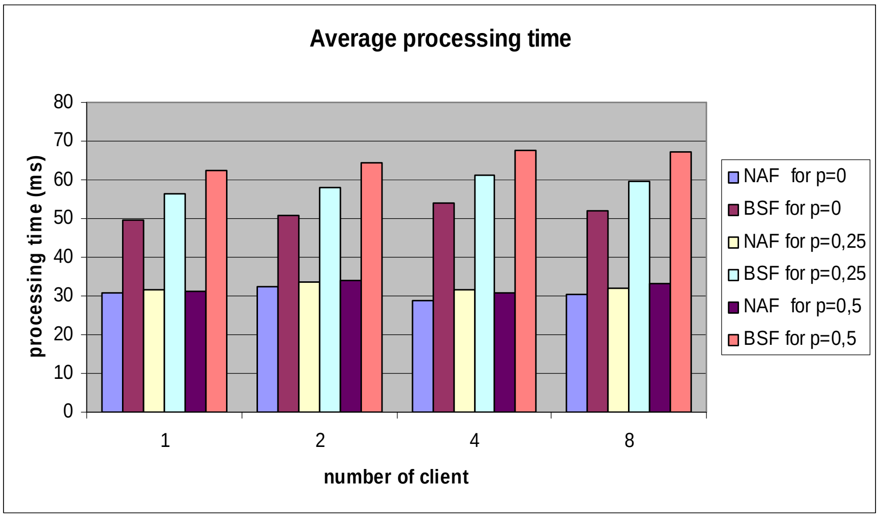


Figure 4-7 Average processing time

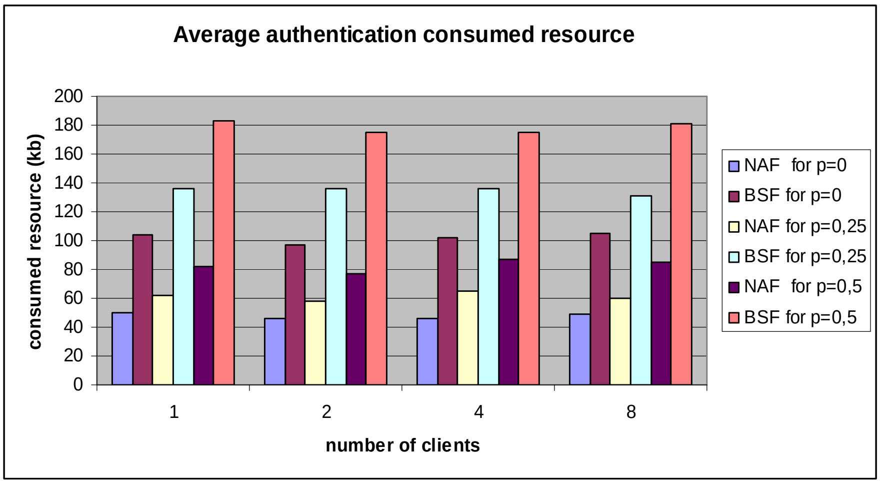


Figure 4-8 Average resources consumption

4.5 Conclusion

This chapter presents a new identification and authentication solution for personalizing IPTV service access. The IBC based service authentication solution (SA-IBC) employs the RFID to identify the user and Identity Based Cryptography (IBC) to allow the personalization of service access through authenticating users in a personal manner during services access. The proposed solution is implemented on top of emulated GBA architectures. Regarding the performance of the proposed solution, the resources consumed during the authentication, and the processing time on servers are measured. The processing time on servers reflect the load imposed during the public key generation. It is observed that the increase in the number of clients does not influence the request average processing time and the average consumed resources. It is also noticed that the processing time on servers and the consumed resources increase with the increase of the authentication failure probability. Finally, it is observed that the BSF represents a bottleneck during the process of service authentication. The following chapter presents an optimization algorithm for decreasing the load on the BSF.

Chapter 5 SA-IBC Modelling and Performance improvement

5.1 Introduction

Considering the big growth of the telecom services, servers need to cope with huge number of users' demands. Since a single server for each service can no longer satisfy the services requirements and could not guarantee a satisfactory quality of experience (QoE) for users. At the same time, performance is an important factor to be considered during users' access to services and hence during the design of authentication and access control protocol. Employing mathematical models to analyze the performance of authentication and access control protocols has not yet received much more attention. In [Harbitter 02] a methodology based on closed queuing network model is proposed to analyze the performance of authentication protocols through considering the customers circulating among the servers with three steps: waiting for services, consuming processing resources, and proceeding to the next service station. In [Liu 08], the authors use a four-dimensional embedded Markov chain to find the stationary probability distribution and find analytical results for several interesting performance metrics. Open BCMP (Baskett Chandy Muntz Palacios) queuing network [Baskett 75] is a multi-class network which is flexible and effective in modeling and evaluating the performance of computer systems. In this chapter, the Open BCMP queuing network is applied to model the SA-IBC identification and authentication solution and analyze its performance.

For performance improvement, the clustering (grouping a series of servers) appears as a promising approach to improve the performance of the SA-IBC authentication solution and hence the whole service. Accordingly, a clustering algorithm is proposed to extend the SA-IBC architecture and the BCMP queuing network is used to model the SA-IBC authentication solution with the proposed clustering algorithm. It is noticed that the proposed clustering algorithm presents an improvement in the performance.

5.2 Overview of BCMP queuing network

The BCMP queuing network has been widely used to evaluate the statistical performance of computer systems and communication networks. The open BCMP queuing network consists of N (N>=1) service centers, which represent the servers or processors in a system. The customers enter the system from the outside, pass from service centre to another, competing for the processing resources of a service center with the other customers at that center, and eventually leave the system. There are R (R>=1) different classes of customers, where customers in different classes require different services and consume different processing resources. Each customer may change from one class to another when changing service centers according to a transition probability.

BCMP queuing network considers four types of service centers: 1) There is a single server at a service center, the service discipline is "first come first serve", all customers have the same service time distribution at this service center and the service time distribution is a negative exponential; 2) There is a single server at a service center, the service discipline is "processor sharing", and each class of customers may have a distinct service time distribution; 3) The number of servers in the service center is greater than or equal to the maximum number of customers that can be queued at this center and each class of customers may have a distinct service time distribution; 4) There is a single server at a service station, the service discipline is "last come first service", and each class of customers may have a distinct service time distribution.

The system state is defined as the number of each class of customers in each service center. So state S of the system is given by (s1,s2,...,sN) where si = (nil,ni2,…,niq) denotes the state of each service center i and niq is the number of customers of class q in service center i. From the BCMP theorem [Baskett 75], the state probability distribution in a BCMP network has the following form:

$$p(n) = cd(n)g_1(y_1)g_2(y_2)\ldots g_m(y_m) \qquad (1)$$

where

$$g(y_i) = \begin{cases} \dfrac{n_i!}{\mu_i^{n_i}}\left[\prod_{q=1}^{Q}\dfrac{\lambda_{i,q}^{n_{i,q}}}{n_{i,q}!}\right] & \text{Service centres of type 1} \\[2ex] n_i!\prod_{q=1}^{Q}\dfrac{\lambda_{i,q}^{n_{i,q}}}{\mu_{i,q}^{n_{i,q}}\, n_{i,q}!} & \text{Service centres of type 2 and 4} \\[2ex] \prod_{q=1}^{Q}\dfrac{\lambda_{i,q}^{n_{i,q}}}{\mu_{i,q}^{n_{i,q}}\, n_{i,q}!} & \text{Service centres of type 3} \end{cases}$$

ni is the number of messages at server i, $\mu i,q$ is the service rate at server i for the messages of class q, $\lambda i,q$ is the arrival rate of messages of class q at the server i.

5.3 Modelling SA-IBC through BCMP queuing network

In this section BCMP queuing network is used to model and analyze the performance of the SA-IBC authentication protocol.

Three servers exist in the SA-IBC system (NAF, BSF and HSS) and N clients will request the authentication. The arrival of clients respects a Poisson distribution with arrival rate λ. Each User Equipment (UE) will send an authentication request. The authentication request will follow the process illustrated in Figure 4-5 in chapter 4. From the implementation, it is observed that the increase in the number of clients does not influence the request average processing time and the average consumed resources. So the treatment of message i ($1 \leq i \leq 12$) of UE j ($1 \leq j \leq n$) is identical (in terms of processing delay and allocated resources) to the treatment of the same message of another UE. That means the service rate of a message in a server (NAF, BSF or HSS) is a constant and independent of the number of messages at that server. The messages of each server are classified according to the type of the message. For example, the NAF receives message 1 and message 9 from the UE as well as message 11 from the BSF; and generates message 2, message 10 and message 12. So three classes of messages exist at the NAF server, respectively class 2, class 10 and class 12 (the generated message number is used as the class number). Similarly, there are four classes of message at the BSF server (class 4, class 6, class 8 and class 11) and one class of message at the HSS server (class 5).

It is considered that the UE receives the messages from the servers, and treats it immediately, so there is no queue at the UE. From the point of view of the servers, there are no differences between the UEs. To simplify the modeling of the solution, a virtual entity called Virtual UE (VUE) is proposed to present all the UEs. The VUE treats and sends the messages to the server in place of the UEs, and hence it can be considered as a service center. The messages in the VUE are classified into four classes: class 1, class 3, class 7 and class 9. UE requesting authentication is considered as arrival of a request to the VUE. Figure 5-1 represents the BCMP modeling for SA-IBC. There are four service centers, VUE, NAF, BSF and HSS. In each service center, there are several classes of messages and each class is named by the sequence number of the generated message. Messages in the service centers are served using processor sharing and messages of different classes have different service rate. In this open queuing network model, the arrival rate of a request to the VUE is denoted by λ and does not depend on the state of the model. So equation (1) can be simplified as:

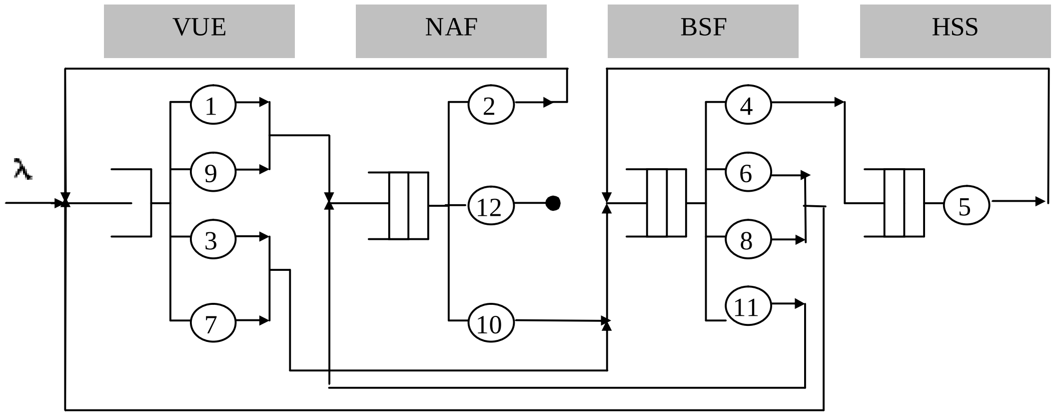


Figure 5-1 Queuing Network Topology

$$p_i(n_i) = (1 - \rho_i)\rho_i^{n_i} \quad (2) \qquad \text{where} \qquad \rho_i = \sum_{q \in Q_i} \frac{\lambda_{i,q}}{\mu_{i,q}} \quad (3)$$

ni is the number of messages at server i, μi,q is the service rate at server i for the messages of class q, λi,q is the arrival rate of the messages of class q to the server i.

In the following subsection, the service utilization and the service authentication delay which are defined in Chapter 4 for SA-IBC are modeled.

5.3.1 Server Utilization

The server utilization is the proportion of time in which the server is busy. It presents the traffic intensity of each server. Equation (3) gives a general formula for the server utilization.

Since an authentication failure may happen even when having a UE belonging to a legitimate user because of transmission errors or different attacks, the authentication failure case is considered. In the case of authentication failure, the authentication process will stop at message 8, in which the BSF sends an authentication failure message to the UE, and the UE will restart the authentication by sending message 1. We denote the failure probability by P_{AF}. Besides the authentication failure, the packet may be lost during the transmission. We denote the packet loss probability by P_l. The packet loss may happen in any message transmission. So from the queuing network topology presented in the Figure 5-1, we can derive transmission probability from class r to class s as follows:

$$p_{t_{r,s}} = \begin{cases} 1-P_l & \text{where } r \neq 8 \text{ and } s = i+1 \\ (1-P_l)(1-P_{AF}) & \text{where } r = 8 \text{ and } s = 9 \\ P_{AF}(1-P_l) & \text{where } r = 8 \text{ and } s = 1 \\ 0 & \text{others} \end{cases}$$

And the arrival rate of the message in each class q is derived as:

$$\lambda_q = \begin{cases} \dfrac{\lambda(1-p_l)^{q-1}}{1-p_{AF}(1-p_l)^8} & \text{where } 1 \leq q \leq 8 \\ \dfrac{\lambda(1-p_l)^{q-1}(1-p_{AF})}{1-p_{AF}(1-p_l)^8} & \text{where } 9 \leq q \leq 12 \end{cases} \quad (4)$$

For simplicity, the packet loss probability is considered small and is ignored. Thus the arrival rate for each class in a simple form is as follows:

$$\lambda_q = \begin{cases} \dfrac{\lambda}{1-p_{AF}} & \text{where } 1 \leq q \leq 8 \\ \lambda & \text{where } 9 \leq q \leq 12 \end{cases} \quad (5)$$

From equation (3) and (5) the server utilization for NAF, BSF and HSS is as:

$$\rho_{NAF} = \lambda\left[\frac{1}{(1-p_{AF})\mu_2} + \frac{1}{\mu_{10}} + \frac{1}{\mu_{12}}\right] \quad (6)$$

$$\rho_{BSF} = \frac{\lambda}{1-p_{AF}}\left[\frac{1}{\mu_4} + \frac{1}{\mu_6} + \frac{1}{\mu_8} + \frac{1-p_{AF}}{\mu_{11}}\right] \quad (7)$$

$$\rho_{HSS} = \frac{\lambda}{(1-p_{AF})\mu_5} \quad (8)$$

5.3.2 Service authentication delay

The service authentication delay (D) is defined as the consumed time from the first authentication request (T0: message1) sent by the UE to the NAF until the reception time of the authentication result (T1). The latter could be a successful authentication message from the

NAF (message 12) or an unauthenticated message from the BSF indicating the authentication failure (message 8) as illustrated in Figure 4-5. The delay is composed of: the time spent on the client, the NAF, the BSF and the HSS (Tc, TsNAF, TsBSF, TsHSS) which includes service processing time and the waiting time in the queuing as well as the authentication request message transmission time (Tt). The service authentication delay D is calculated as follows:

$$D = T1 - T0 = Tc + Ts_{NAF} + Ts_{BSF} + Ts_{HSS} + Tt \qquad (9)$$

According to the assumption of the VUE, there is no queuing in the VUE. The waiting time in VUE is then equal to 0. So:

$$Tc = \sum_{q \in Q_{VUE}} \frac{1}{\mu_q} \qquad (10)$$

where Q_{VUE} = {class1, class3, class7, class9}, μq is the service rate for the messages of class q.

From equation (2), the average number of customers at the service centers NAF, BSF or HSS is calculated as follows:

$$E(n_i) = \sum_{n_i = 1}^{\infty} n_i p_i(n_i) = \frac{\rho_i}{1 - \rho_i} \qquad (11)$$

where i={NAF,BSF,HSS}, ni is the number of messages at server i.

According to the LITTLE Formula[Leon-Garcia 08], the service delay at each service center NAF, BSF, or HSS is:

$$T_i = \frac{E(n_i)}{\lambda_i} = \frac{E(n_i)}{\sum_{q \in Q_i} \lambda_{i,q}} = \frac{\rho_i}{(1 - \rho_i)\sum_{q \in Q_i} \lambda_{i,q}} \qquad (12)$$

We substitute by (10) and (12) in equation (9) to calculate D:

$$D = \sum_{q \in Q_{VUE}} \frac{1}{\mu_q} + Tt + \sum_i \frac{\rho_i}{(1 - \rho_i)\sum_{q \in Q_i} \lambda_{i,q}} \qquad (13)$$

where i={NAF,BSF,HSS}, $\lambda i,q$ is the arrival rate of the messages of class q to the server i and calculated from equation (5). ρi is the server utilization for NAF,BSF and HSS and calculated from equations (6) to (8).

5.4 Proposed Clustering Algorithm

Clustering is emerging as a valuable architecture to improve the network performance. With the increase of users' requests, a single centralized server at NAF, BSF and HSS no longer satisfies the service requirements and could not guarantee a satisfactory QoE. In order to improve the performance of services and to prevent any bad impact due to authentication and access personalization, a clustering solution is proposed introducing more servers at NAF, BSF and HSS considering that all the servers have the same capacity for simplicity. The number of servers at the NAF, BSF and HSS are denoted by N_{NAF}, N_{BSF}, N_{HSS}. So the service rate for each message of class q will increase and the new service rate will become: $N_{NAF}\mu q$ (if class q is at NAF), $N_{BSF}\mu q$ (if class q is at BSF) and $N_{HSS}\mu q$ (if class q is at HSS). The new server utilization for NAF, BSF and HSS which is denoted by $\rho i'$ becomes:

$$\rho_i' = \frac{\rho_i}{N_i} \qquad i=\{NAF,BSF,HSS\} \tag{14}$$

From equations (13) and (14) the new delay for the clustering system is given as.

$$D = \sum_{q \in Q_{VUE}} \frac{1}{\mu_q} + Tt + \sum_i \frac{\frac{\rho_i}{N_i}}{\left(1 - \frac{\rho_i}{N_i}\right) \sum_{q \in Q_i} \lambda_{i,q}} \tag{15}$$

5.4.1 Intelligent clustering algorithm

For better performance and scalability the amount of resources (number of servers) should be proportional to the charge. An intelligent clustering algorithm is then proposed which distributes the servers in an intelligent manner considering the service rate.

It is supposed that there are C (C is a constant) servers in total. So:

$$N_{NAF} + N_{BSF} + N_{HSS} = C \tag{16}$$

Equation (15) presents the delay of the authentication process which also presents the performance of the whole system. The third element of equation (15) reflects the relationship between the delay and the number of the servers at the NAF, BSF and HSS. The servers distribution proportion among the N_{NAF}, N_{BSF} and N_{HSS} is calculated allowing to have the minimum delay value. From the arithmetic mean-geometric mean (AM_GM) inequality, any list of n nonnegative real numbers: $x_1, x_2, \ldots, x_n$, satisfies the following inequality:

$$\frac{x_1 + x_2 + \ldots + x_n}{n} \geq \sqrt[n]{x_1 . x_2 \ldots x_n}$$

and that equality holds if and only if $x1 = x2 = \ldots = xn$.

Since the service rate μ of each server and the transmission time do not change, to have the minimum authentication delay, third element of equation (15) have to attain its minimum value. According to the arithmetic mean-geometric mean (AM_GM) inequality [Steele], the minimum delay value is:

$$\sum_{q \in Q_{VUE}} \frac{1}{\mu_q} + Tt + \sum_i \frac{\frac{\rho_i}{N_i}}{\left(1 - \frac{\rho_i}{N_i}\right) \sum_{q \in Q_i} \lambda_{i,q}}$$

$$= \sum_{q \in Q_{VUE}} \frac{1}{\mu_q} + Tt + \sum_i \frac{\rho_i}{(N_i - \rho_i) \sum_{q \in Q_i} \lambda_{i,q}}$$

$$= \sum_{q \in Q_{VUE}} \frac{1}{\mu_q} + Tt + \frac{C - \sum_i \rho_i}{C - \sum_i \rho_i} \sum_i \frac{\rho_i}{(N_i - \rho_i) \sum_{q \in Q_i} \lambda_{i,q}}$$

$$= \sum_{q \in Q_{VUE}} \frac{1}{\mu_q} + Tt + \frac{\sum_i (N_i - \rho_i)}{C - \sum_i \rho_i} \sum_i \frac{\rho_i}{(N_i - \rho_i) \sum_{q \in Q_i} \lambda_{i,q}}$$

$$\geq \sum_{q \in Q_{VUE}} \frac{1}{\mu_q} + Tt + \frac{1}{C - \sum_i \rho_i} \left(\sum_i \frac{\rho_i}{\sum_{q \in Q_i} \lambda_{i,q}} + 2 \sqrt{\frac{\rho_{NAF}\, \rho_{BSF}}{\sum_{q \in Q_{NAF}} \lambda_{NAF,q} \sum_{q \in Q_{BSF}} \lambda_{BSF,q}}} \right.$$

$$\left. + \; 2 \sqrt{\frac{\rho_{NAF}\, \rho_{HSS}}{\sum_{q \in Q_{NAF}} \lambda_{NAF,q} \sum_{q \in Q_{HSS}} \lambda_{HSS,q}}} + 2 \sqrt{\frac{\rho_{BSF}\, \rho_{HSS}}{\sum_{q \in Q_{BSF}} \lambda_{BSF,q} \sum_{q \in Q_{HSS}} \lambda_{HSS,q}}} \right)$$

The minimum delay value can be obtained if and only if N_i (i={NAF,BSF,HSS}) satisfies the following condition:

$$N_{NAF} = \frac{\sqrt{\frac{\sum_{q\in Q_{BSF}} \lambda_{BSF,q} \sum_{q\in Q_{HSS}} \lambda_{HSS,q}}{\rho_{BSF}\rho_{HSS}}}\left(C-\sum_i \rho_i\right)}{A} \quad (17)$$

$$N_{BSF} = \frac{\sqrt{\frac{\sum_{q\in Q_{NAF}} \lambda_{NAF,q} \sum_{q\in Q_{HSS}} \lambda_{HSS,q}}{\rho_{NAF}\rho_{HSS}}}\left(C-\sum_i \rho_i\right)}{A} \quad (18)$$

$$N_{HSS} = \frac{\sqrt{\frac{\sum_{q\in Q_{NAF}} \lambda_{NAF,q} \sum_{q\in Q_{BSF}} \lambda_{BSF,q}}{\rho_{NAF}\rho_{BSF}}}\left(C-\sum_i \rho_i\right)}{A} \quad (19)$$

Where

$$A=\sqrt{\frac{\sum_{q\in Q_{NAF}} \lambda_{NAF,q} \sum_{q\in Q_{BSF}} \lambda_{BSF,q}}{\rho_{NAF}\rho_{BSF}}}+\sqrt{\frac{\sum_{q\in Q_{BSF}} \lambda_{BSF,q} \sum_{q\in Q_{HSS}} \lambda_{HSS,q}}{\rho_{BSF}\rho_{HSS}}}+\sqrt{\frac{\sum_{q\in Q_{NAF}} \lambda_{NAF,q} \sum_{q\in Q_{HSS}} \lambda_{HSS,q}}{\rho_{NAF}\rho_{HSS}}}$$

Since the total number of the servers is constant, from equations (17), (18), and (19) the servers distribution proportion is derived among N_{NAF}, N_{BSF} and N_{HSS} that allows to attain the best performance as shown in equation (20):

$$N_{NAF} : N_{BSF} : N_{HSS} = \sqrt{\frac{\sum_{q\in Q_{BSF}} \lambda_{BSF,q} \sum_{q\in Q_{HSS}} \lambda_{HSS,q}}{\rho_{BSF}\rho_{HSS}}} : \sqrt{\frac{\sum_{q\in Q_{NAF}} \lambda_{NAF,q} \sum_{q\in Q_{HSS}} \lambda_{HSS,q}}{\rho_{NAF}\rho_{HSS}}} : \sqrt{\frac{\sum_{q\in Q_{NAF}} \lambda_{NAF,q} \sum_{q\in Q_{BSF}} \lambda_{BSF,q}}{\rho_{NAF}\rho_{BSF}}} \quad (20)$$

From equations (5) to (8), it is found that $\lambda i,q/\rho i$ (where i={NAF,BSF,HSS})is no longer function of λ, however it is the function of service rate μq of each message q. Consequently the servers distribution proportion among the N_{NAF}, N_{BSF} and N_{HSS} is determined by the service rate μq in the NAF, BSF and HSS. So the number of the servers in the NAF, BSF and HSS is directly proportional to the service rate in these latter. From equations (16) and (20), the number of servers can be calculated at the NAF, BSF and HSS. And, from equations (14) and (15) the corresponding server utilization and service authentication delay are calculated.

5.5 Performance Analysis

For analyzing the performance of the SA-IBC solution in a scalable manner, the derived BCMP model is implemented under MatLab [Matlab] and the server utilization and the service authentication delay are calculated under different client arrival rates. A performance comparison is carried out between the single server system and the clustering system. For message transmission time and the service rate parameters in the model, the values obtained from the implementation previously carried out are used [Song 11]. Authentication failure probability is defined as: P_{AF} = 0.05, which presents 5% failure among the clients wishing to authenticate. For the clustering system, the performance of two different clustering approaches having a similar total number of servers is analyzed:

1) clustering system A in which the servers distribution does not consider the service rate of the system (considering the same number of servers for the NAF, BSF and HSS),

2) clustering system B in which servers distribution at the NAF, BSF and HSS depends on the service rate.

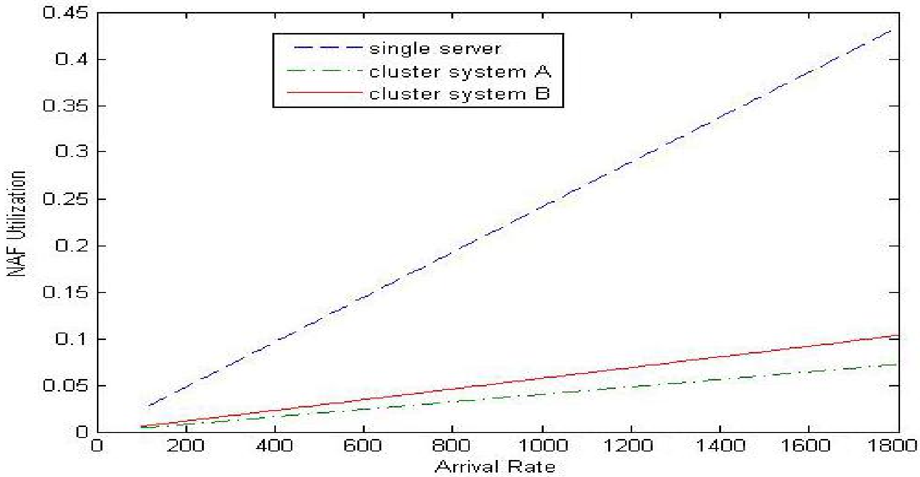


Figure 5-2 NAF Utilization

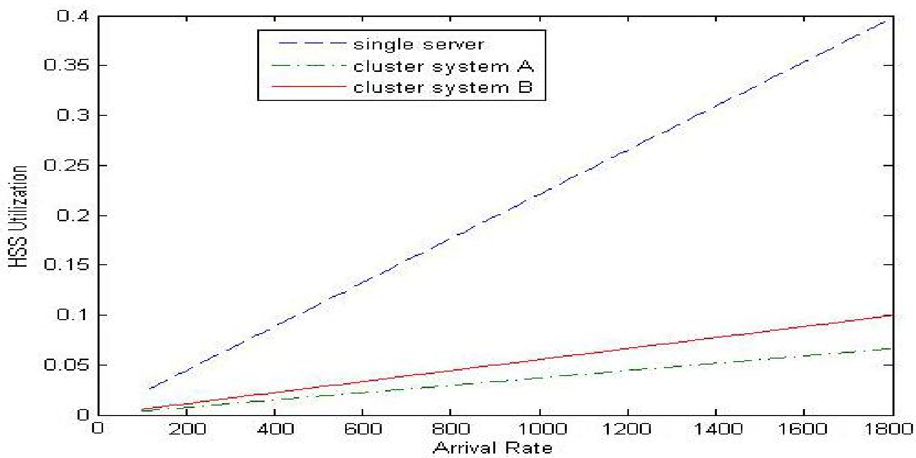


Figure 5-3 HSS Utilization

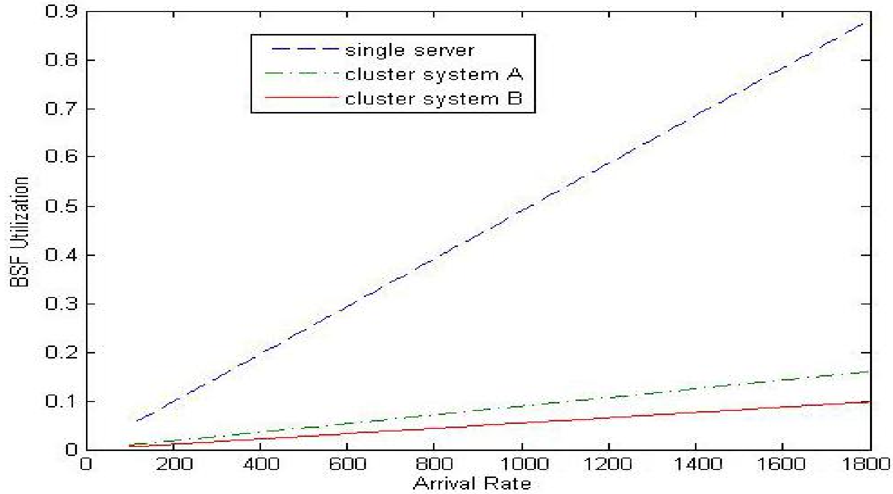


Figure 5-4 BSF Utilization

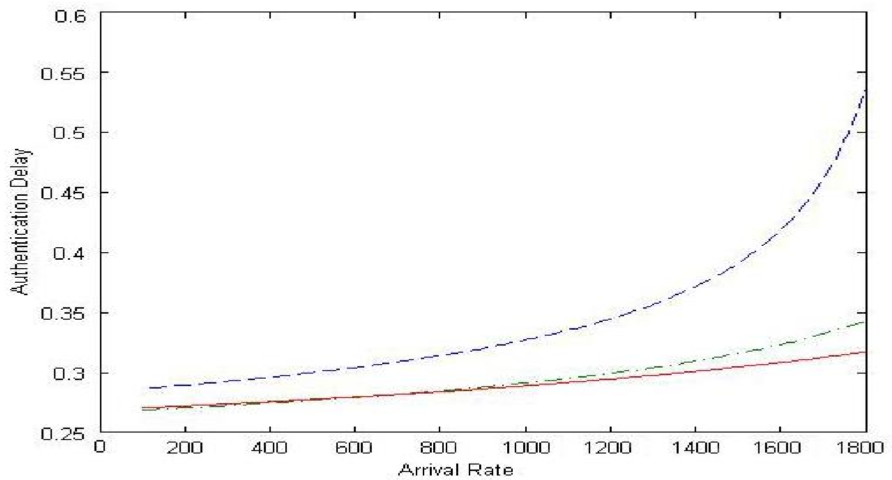


Figure 5-5 Authentication Delay

Figures 5-2, 5-3 and 5-4 respectively presents the server utilization for the NAF, BSF and HSS. An increase of the server utilization is observed when the arrival rate λ rises. This increase is slower with clustering.

In the single server case, the server utilization increase in the BSF is more rapidly than that in the NAF and HSS since the BSF processes more HTTP messages and carries out more encryption/decryption calculation (presenting a bottleneck in the service authentication process).

Comparing the two clustering systems A and B, the server utilization of system B is bigger than that of system A for the NAF and HSS and vice-versa for the BSF. That's because in system B, the servers distribution is realized through considering the service rate in the NAF, BSF and HSS with fewer servers at the NAF and HSS and more servers at the BSF compared to system A. In system A, the server utilization increase in the BSF is still more rapid than that in the NAF and HSS. However, in system B, the server utilization of the NAF, BSF and HSS is almost similar. The BSF is no longer the bottleneck. So the whole performance of system B is better than system A.

Figure 5-5 illustrates the average service authentication delay with different arrival rates. The delay increases when the arrival rate rises. This is mainly due to the load rising on the NAF and the BSF, causing more delay in processing the service authentication requests. This increase is slower in the clustering system A and B, especially in system B which shows better performance.

5.6 Conclusion

This chapter considers Open BCMP queuing network as a mathematical model to evaluate the performance of SA-IBC authentication solution in a scalable manner. A clustering algorithm is also proposed to improve the performance of the authentication solution through distributing the servers within the SA-IBC architecture according to the service rate of the system. The BCMP model for SA-IBC is implemented under Matlab with and without the proposed clustering algorithms and the performance is evaluated through measuring the service utilization and authentication delay in the presence of large number of client. It is observed that the increase in the number of clients has an impact on the server utilization and authentication delay. Furthermore, it is observed that the BSF presents a bottleneck in the process of service authentication, where the proposed clustering algorithm proved to improve the performance of the system.

Part III Context-awareness based Content Recommendation for IPTV services

Chapter 6 Context-aware IPTV Content Recommendation Service

With the expansion of TV content, digital networks and broadband, hundreds of TV programs are broadcast at any time of day. Users need to take a long time to find a content in which he is interested. This problem is known in literature as content overload. It becomes a major challenge for computing research in the coming years, the development of customized solutions to access and manage large volumes of information and multimedia content. In this context, the strategy of personalized content recommendation is being used by recommender systems as a possible solution to cope with this problem by automatically matching user's interests to TV programs and recommending the ones corresponding to high user's interests.

6.1 Introduction and Related work and Problem Statement

Recommendation systems are powerful tools that can help the user to address the problem of information and content overload by guiding him in a personalized way to select useful objects from a wide range of possible options. Based on how recommendations are made, recommendation systems apply three approaches [Adomavicius 05]: 1) Content-based recommendation: compares the descriptions of content contained in documents with the interest specified in the user profile. The user will be recommended items similar to his interest or the ones the user watched in the past. 2) Collaborative recommendation: The recommendation system identifies users who share the same preferences (e.g. rating patterns) with the active user. Usually, a viewing community is generated whose members share similar viewing preferences or similar viewing habits. The user will be recommended items that are consumed by people with similar preferences. 3) Hybrid system: Recommendations are made through the combinations of results of contents based recommendation and collaboration based recommendation.

A content based recommendation system is proposed in [Yu 03]. In this work, the user's profile and content are defined in terms of vectors of weights of important keywords: like

(WU1, WU2, … WUn) and (WC1,WC2,…WCn), where weight WCi denotes the importance of keyword i to user U, and weight WCi denotes the importance of keyword i to content C. The similarity between the vector of the user profile and the vector of each content vector is calculated. The content which has highest similarity with the user profile is recommended.

A collaboration based recommendation system is proposed in [Chen 09]. In this system, TV programs are classified into different types and the user's viewing habits are described by a vector of the user's watching duration to each program type. The users with similar viewing habits are categorized into one community, and the consumed contents from these similar users are aggregated. For the recommendation, the content that consumed by the community and the target user has not consumed is recommended.

A hybrid approach to generate content recommendation is proposed in [Ardissono]. In this work, three user modeling modules collaborate in preparing the final recommendations: Explicit Preferences Expert, Stereotypical Expert, and Dynamic Expert. The Explicit Preferences Expert deals with preferences declared by the users during service subscription. The Stereotypical Expert exploits users' personal data known to the system and the explicit preferences stated in order to classify individual users into a lifestyle (stereotypical) groups. The Dynamic Expert analyzes users' watching behaviors, and based on it builds the model of the user. During the analysis of user's watching behaviors, the authors consider the influence of time to user's preference. However, other context information like location is not considered. The Personalized Electronic Program Guide (EPG) is generated through mixing the results of the three user modeling modules.

It is noticed that traditional content recommendation systems consider only the user's preference and consumed history as the criteria while the general context information is not considered (like device capacity, network states, location, time, user's activity…etc). However, the general context information takes an important role for the recommendation service because the user's preference on IPTV content is not fixed and it changes depending on certain context such as time, location, activity, etc. Furthermore, certain contents are accessible based on some conditions. For example only the device which supports the High Definition (HD) could display the HD film. If a user chooses to watch TV through a terminal which does not support HD, the recommendation system should not propose the HD content for him supposing that no Simple Definition 'SD' content is available for this same content.

The service recommendation also attracted the attention of the IPTV standards. Within the ETSI/TISPAN Standard, it is proposed that the recommendation may take the form of a text message (notification) from CFIA (Customer Facing IPTV Application) or video recommendation streamed from MDF (Media Delivery Function). Within the CRS (Content Recommendation Service) entity two functions are proposed:

1) Aggregation of metadata for recommendations: (a) user's profile, preferences, etc. b) Asset metadata for Content on Demand (CoD) and linear TV (EPG).

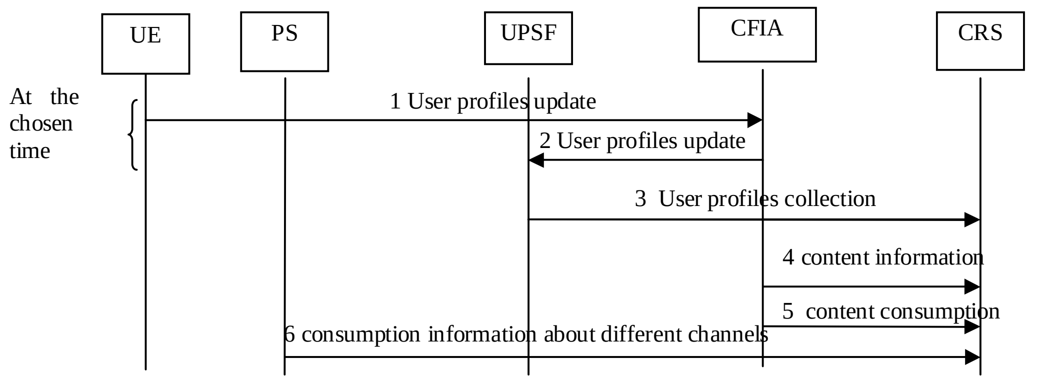


Figure 6-1 Aggregation of metadata for recommendation service

2) Generation of recommendations upon request of external triggers: (a) a user sends service request, b) changes in the user's presence state).

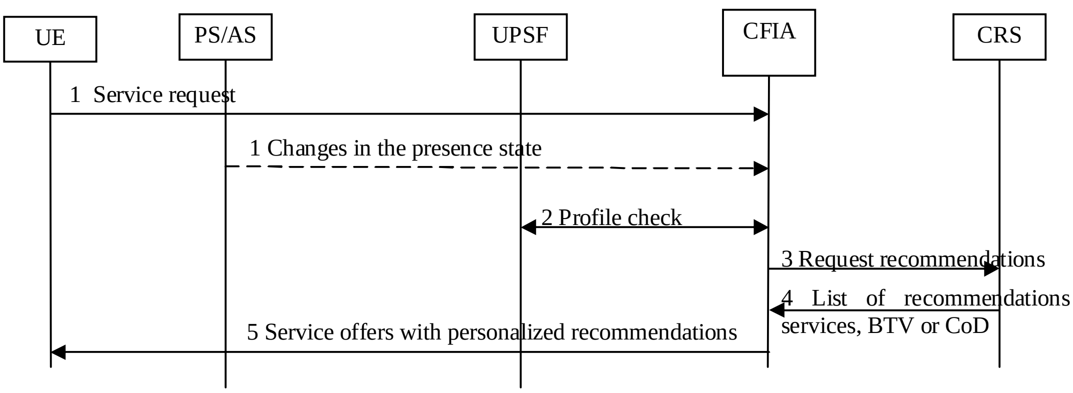


Figure 6-2 Recommendation request and delivery

The chapter proposes an enriched personalized recommendation system which improves the quality of recommendation by analyzing user preferences and his access to the content based on the global context information of the user and his environment.

6.2 General overview of the proposed content recommendation system

The recommendation systems use effective information such as demographics, preferences, to select items that are likely to interest the user. Thus, it becomes necessary to collect and store the information to be used later in the process of recommendation.

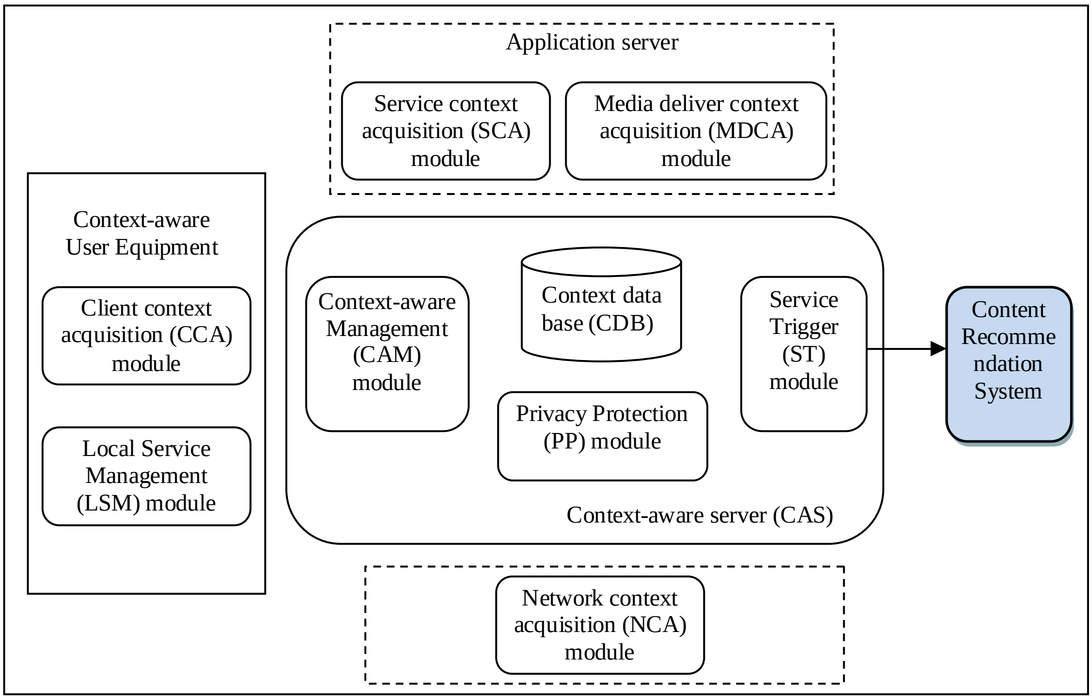


Figure 6-3 Context-awareness based recommendation system

The proposed context-aware IPTV recommendation system recommends the content to users not only considering the user's preference (it considers the user's preference as part of the user context) but also the other context information. So the context information is considered as the metadata for the proposed recommendation system. In chapter 3, four types of contexts are considered in IPTV services: i) User Context: Includes information about the user, which could be static information and dynamic information. The static information describes the user's personal information which is stored in the user profile database (ex, name, age, sex, and input preference). The dynamic information is captured by sensors or by other services (ex, user's location, time, consumption history). ii) Device/Terminal Context: Includes information about the devices (terminals), which could be the device identity, status (turn on or off, volume), device capacity, and the device proximity to the user. iii) Network Context: Includes information about the network as the bandwidth, delay, jitter, the network load, and the user subscription type with respect to the access network. iv) Service Context: Includes information about the service, which could be the content description (type of the content, director, actors) and service description (like content format, language, etc). These four types of context are firstly collected by the context-aware server proposed in chapter 4. Then the service trigger module triggers the content recommendation system as illustrated in Figure 6-3.

6.3 Metadata for recommendation

According to the use of the context information, the metadata for context-aware recommendation is divided into two categories:

1) Conditional Context: the context information that decides whether the contents are accessible or allowed to be accessed by user before doing the content recommendation. Taking the device capacity as an example: if a device only supports SD (Standard Definition) (device capacity), so user could not access the HD (High definition) content through this device. The conditional context information includes device capacity, network capacity and user's age.

2) Situational Context: the context information that influences the user's preference regarding two aspects. a) The situational context which includes several context types (location, time, etc) and each context type has several context values influencing user's preferences. Taking 'TIME of the Day' as an example: user likes to watch news at 20 o'clock, while at 23 o'clock he likes watching movies. b) Different context types have different influence levels on the user's preference. For example, considering two context types time and location (time interval 4 = o’clock & user’s location = salon) as the user’s current context and having the following cases:

- The user hardly watches TV at 4 o'clock but likes to watch News if he decided to watch TV at 4 o’clock.
- This user frequently watches TV in the salon but likes to watch films most of the time when he is in the salon.

Consequently, for the current context in which a user is in the salon at 4 o’clock, the context “location” has more impact on the preference degree of the user than the context “time = 4 o'clock”. Then, the content feature associated with the presence of the user at the salon (Films in this example) is highly recommended.

To reflect the impact of the context information on the user’s preference, the following parameters are calculated and used during the generation of recommendation:

1) Preference degree for a content feature at a context value:

$$\text{Preference degree for content feature i at the context value v} = \frac{\text{Duration of watching the content feature (i) within the context value (v)}}{\text{Duration of watching TV during an observation period within the context value v}}$$

2) Influence degree for a context value:

$$\text{Influence degree for a context value v} = \frac{\text{Duration of watching TV within a context value (v)}}{\text{Total consumption duration during an observation period}}$$

6.4 Generation of recommendation

According to the classification of the context information, two modules are proposed in the recommendation system.

6.4.1 Static content filtering module

A rule-based approach is applied by this module to evaluate contents and to filter out the contents which do not match the conditional context information. Based on the stored rules and the conditional context information, this module determines which content is not supported by the device or network or not permitted to be accessed by the user.

6.4.2 Dynamic content ordering module

This module applies a layered based approach having weighted connections between layers, inspired from the Neural Networks [Hudson 03], to evaluate the contents against the Situational Context, however using the user's feedback in real time to dynamically update the weight values between the layers. Each layer contains several nodes and each node performs its own computations for the context information processing. With the interaction (weighted connection) between the nodes in different layers, the approach is capable of performing powerful computations by combining the processing power of all the nodes.

a) Layering approach:

There are three layers in this approach and each layer performs a specific function. Figure 6-4 illustrates this layered based approach.

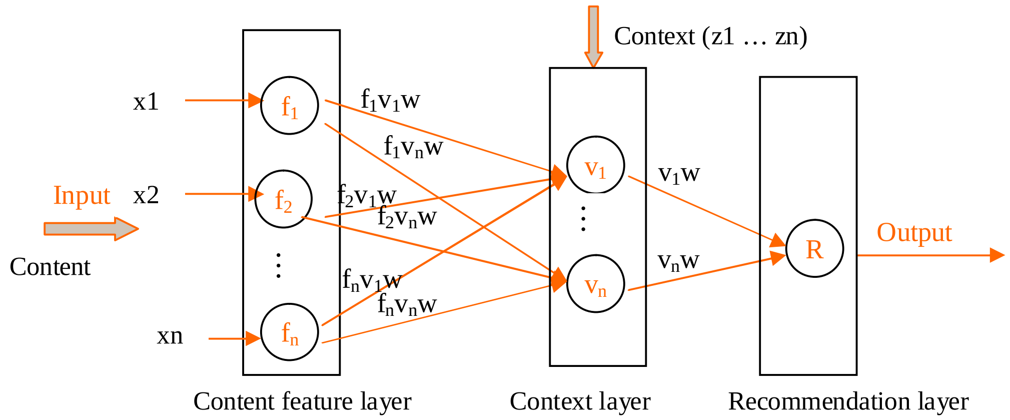


Figure 6-4 Layer based approach

The first layer is the content feature layer. Each node in this layer presents a content feature. The second layer is the context layer. Each node in the context layer represents a context value. This layer is fully connected to the content feature layer. Wfivj is the weight value between a node in the content feature layer (fi) and a node in the context layer (vj) and presents the user's preference degree for a content feature fi at a context value vj. The third layer is the recommendation layer which has the role of calculating the recommendation rating of the input content and contains only one node (R). This layer is fully connected to the context layer. Wvir is the weight value between a node in the context layer (vi) and a the node of recommendation layer (R) and presents the influence degree for a context value vi.

The content feature layer takes the content as an input vector describing the content. An item of the vector corresponds to a feature node of the content feature layer. The value of each item is assigned to 0 or 1 (the value ‘0’ signifies that the content does not have the corresponding feature while the value '1' signifies that the content has the corresponding feature). For example, if only first two items of a content vector equal to 1, and the rest equal to 0 (like [1,1, 0 … 0]), that means this content only possesses the first two features of the content feature layer. The nodes at the content feature layer use the following convert function to generate the output:

$$g_i = f_i x_i \qquad (1)$$

Where f_i is the initial value for each feature node (and each feature node f_i is initialized by the value ‘1’), x_i is the input value for the feature node f_i and g_i is the output of the content feature node f_i to the context value node in the context layer.

The weighted output of the feature layer to the node v_j in the context layer is calculated as follows:

$$\sum_{i=1}^{n} g_i * f_i v_j w \qquad (2)$$

The context layer node v_j takes the weighted output of the feature layer and the context as input. A vector is used to describe the current context, where an item of the vector corresponds to a context value node of the context layer. The value of each item is assigned to 0 or 1 (the value '0' signifies that that the current context does not have the corresponding context value

while the value '1' signifies that the current context has the corresponding context value). The convert function for the context value node is calculated as follows:

$$q_j = \left(\sum_{i=1}^{n} g_i * f_i v_j w \right) * z_j \qquad (3)$$

where zj is the input for the context value node vj; fivjw is the weight for the connection between a node in the content feature layer fi to a node in context layer vj; qj is the output of the context value node vj to the recommendation node R;

The recommendation node in the recommendation layer aggregates the weighted output of the context layer and generates the final rating score (S) for the input content vector. This score reflects the user's preference level to the input content at the current context. According to the scores of all the contents, the system could generate a recommendation list which contains the contents with the first three highest scores.

$$s = \left(\sum_{j=1}^{m} q_j * v_j w \right) \qquad (4)$$

where vjw is the weight for the connection between a node of context layer vi and the node of recommendation layer R. S is the final rating score for the input content.

b) Weight value learning and update

As described above, the connection weight values between the content feature layer and the context layer present user's preference degree for different content features at different context values; and the connection weight values between the context layer and recommendation layer respectively reflects the influence degree for different context values on the user's preference. According to user's feedback on the contents in the recommendation list, the recommendation system updates the connection weight values automatically. The user's feedback is calculated in an implicit mean through analyzing the user's watching duration based on the previously defined preference and influence degrees, which avoids disturbing the user and asks him to explicitly give his rating score. The user's feedback is then used in the weight values update as follows:

$$f_i v_j w = \left(f_i v_j w' + \frac{\text{Duration of watching the content feature } (f_i) \text{ of current day within the context value } (v_j)}{\text{Duration of watching TV of today in the context type } v_j} \right) * 1/2 \quad (5)$$

fivjw ' is the old weight value

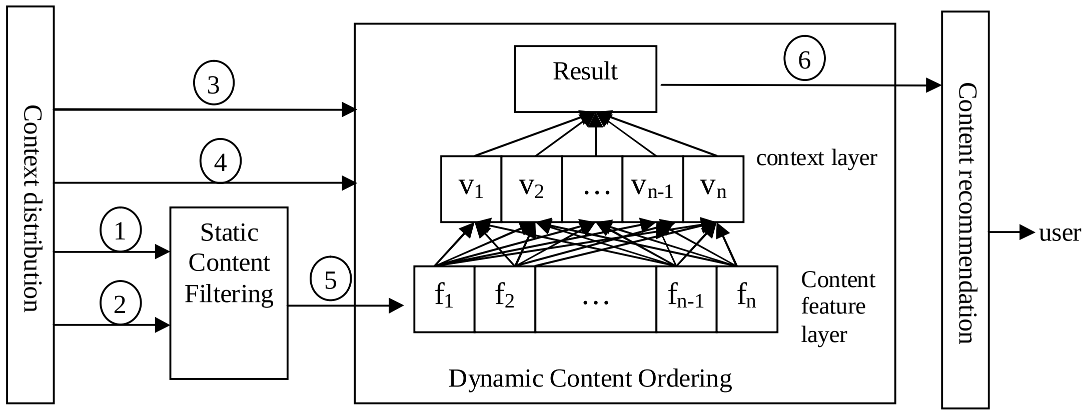
$$v_j w = \left(v_j w' + \frac{\text{Duration of watching TV within a context value (vi) of current day}}{\text{Duration of watching TV of current day}} \right) * 1/2 \quad (6)$$

$v_j w$ ' is the old weight value

These weight values could be updated once a day or at the end of each service session. This depends on the implementation choice.

6.5 Architecture of the context-aware recommendation system

Using the static content filtering solution and the dynamic content ordering solution, a context-aware IPTV recommendation system is built benefiting from the context-aware server for the context information acquisition as explained in section 6.2. This system comprises four components as showing in figure 6-5: context distribution module, content filtering module, content ordering module and content recommendation:



1: content context information
2: conditional context information
3: situational context information
4: Preference degree for the content feature at a context value and Influence degree for the context value
5: selected content
6: recommendation list

Figure 6-5 Architecture of the context-aware recommendation system

The Context Distribution module acquires the context information from the context-aware server. Then it inputs the content context information and conditional context information to the content filtering module. It also inputs the situational context information and user's Preference degree for the content feature and the influence degree for the context value (connection weights between layers) to the Dynamic Content Ordering module.

The Static Content Filtering module filters the contents compared to the received conditional context. According to the stored rules and the conditional context information, this module filters out the contents not matching the user and forwards the rest to the content ordering module.

After receiving the situational context information and user's Preference degree for the content feature and the influence degree for the context value from the content distribution module and the contents information from the content filtering module, the Dynamic Content Ordering module calculates the rating score for each content following the layered based approach and generates the recommendation list based on the rating score, then it sends the recommendation list to the content recommendation module.

Based on the recommendation list, the content recommendation module generates the personalized Electronic Program Guide (EPG) and sends it to the end user.

6.6 Content recommendation for group of users

Recommendation for group of users is also provided by the proposed recommendation system. The context distribution module should acquire the user context information of all the users in the group from the context-aware server.

The static content filtering module selects the contents matching all the users and sends them to the dynamic content ordering module.

The dynamic content ordering module calculates the connection weight values between layers for the group of users which presents the group weight value GWfivj for the connection between a node of the content feature layer (fi) and a node of the context layer (vj) and the group weight value GWvir for the connection between a node of context layer (vi) and the node of recommendation layer R.

The average connection weight values of all users in the group are used to present the connection weight values for the group. For example, if there are M users in a group G, each user K has the weight value KWfivj for the connection between a node of content feature layer (fi) and a node of context layer (vj) and the weight value KWvir for the connection between a node of context layer (vi) and the node of recommendation layer R, then the connection weight values GWvir and GWfivj for the group are calculated as:

$$GWf_i v_j = \frac{\sum_{ALLUsers} KWf_i v_j}{M} \qquad (7)$$

$$GWv_j r = \frac{\sum_{ALLUsers} KWv_j r}{M} \qquad (8)$$

The group weight values are used in the dynamic ordering module to calculate the rating score of each content for the group of users and further generate the recommendation list for the group of users.

6.7 Implementation and performance analysis

6.7.1 Implementation

The recommendation system is implemented using the C language and runs on a machine with a 2.4-GHz Pentium 4 CPU, and1 GB of RAM. The HTTP protocol is used between the

Service Trigger module in the Context-aware server and the Context Distribution module in the recommendation system. The context information is encapsulated in the HTTP protocol and follows the XML format defined in chapter 2. In order to allow the Context Distribution module to extract the information from the received HTTP messages, a parser is developed using LEX [Levine 92], which is a tool to generate a program to recognize lexical patterns in text. In the Static Content Filtering module, the "IF-Then" clause is used to define the rules to filter the contents according to the conditional context information.

For the Dynamic Content Ordering, two "one dimensional arrays data structure" are used to respectively present the content feature layer, context layer (Content[N], Context[M]). The index of the array indicate the node and the value of each element presents the corresponding value of each node. For example for the Content[i], the index i presents the node i of the content layer and the value of the element "Content[i]" presents the value of the node i. A "two dimensional arrays data structure" (Connection[N][M]) is used to present the weight values for the connection between the nodes of content feature layer and the nodes of context layer. The index "N" and "M" represent the nodes in the content feature layer and in the context layer and the value of the element presents the weight value of the connection between the nodes. Another "one dimensional arrays data structure" ConnectionCR[M] is used for presenting the weight values of the connection between the nodes of context layer and the node of recommendation layer. The arrays based data structure simplifies the mathematical calculation.

6.7.2 Performance Analysis

During August-September 2011, five users were invited to record their TV watching habits, (watched content, the location and time for watching and the used device such as PC, TV or smart phone) as well as the watching duration about the watched contents. The content context information is collected through XMLTV [XMLTV]. These data sets are divided into two classes: the first class is used by the system to learn the parameters of the system (weight value of each connection between the layers) and the second class is used to evaluate the performance. The Performance evaluation is a core aspect of recommender systems design and deployment. The proposed content recommendation system is evaluated from following two aspects: delay of the recommendation and accuracy of the content recommendation system.

1) Delay of the recommendation, measures the time spent for the recommendation. The content recommendation system is a real-time application especially when considering the user's context information. The recommended contents should follow up the change of the context. So the time factor is crucial, because long delays create negative user experiences.

The recommending time along with the change of the number of movies from 20 to 200 is measured. When a user starts watching TV, the context-aware IPTV activates the content recommendation system, which calculates the rating score of each content viewed in a specific context, and then sends the final recommendation list to the user. The blue line in Figure 6-6 shows the obtained results: the recommendation delay increases proportionally when the number of content increases.

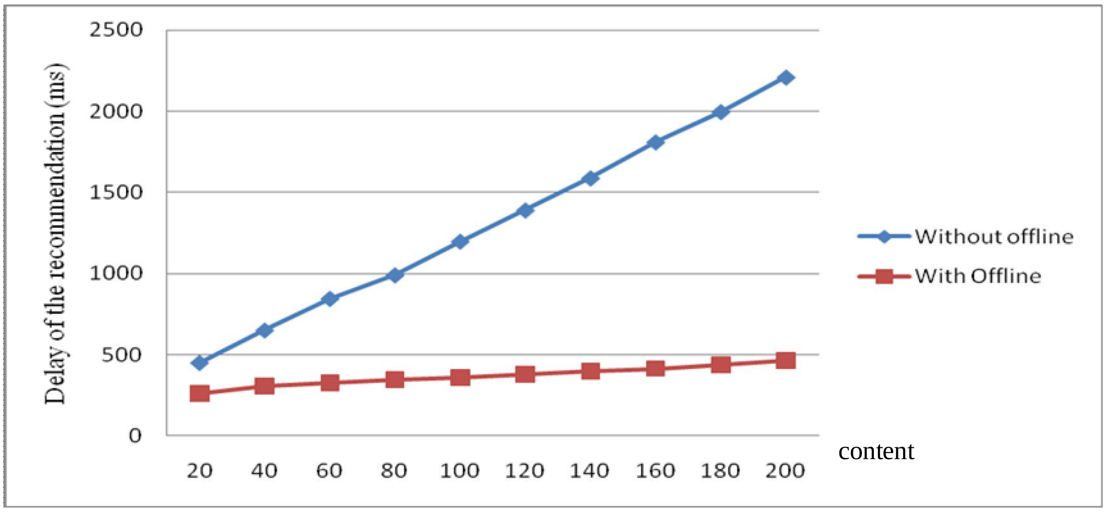


Figure 6-6 Delay of the recommendation

If the content database becomes very large, users have to wait a long time to receive the recommended list which influences the user's quality of experience (QoE). In order to resolve this problem, the recommendation delay is split calculation into offline phase and online phase. The offline phase performs the calculation beforehand while the online phase performs the calculation when the recommendation service is activated.

Offline phase: Considering that the Electronic Program Guide (EPG) is scheduled before the content display and in the implementation the Context-Aware System (CAS) could get the EPG from the Service Context Acquisition (SCA) one day in advance, the weighted output of the Content feature layer in the dynamic content ordering module could be calculated beforehand. To achieves this, the Context Trigger module activates the offline calculation one day in advance at a specific time (0:00 for example), and all the content context information is sent to the content ordering module of the recommendation system. The weighted output of the feature layer to the node in the context layer is calculated through Equation (2) and stored in a database.

Online phase: When a user starts watching TV, the context-aware IPTV actives the content recommendation system and sends the context information to this latter. The Static Content Filtering module filters out the contents that do not match the conditional context and forwards the rest to the content ordering module. Then the dynamic content module retrieves the pre-calculated weighted output of the feature layer for each received content from the database and continues calculating the rating score for each content in the current situation context.

Because the offline computation is always running in the background, and its time was transparent to the user, only the online time was crucial for the performance evaluation. The red line in Figure 6-5 shows the improved result. It is noticed that the delay of the recommendation is much less in the approach with the offline calculation.

2) Accuracy of the content recommendation system. From the user's perspective, the accuracy of the content recommendation system is evaluated which indicates whether the system could recommend the right content to the user and reflects users' satisfaction for a given recommendation. The precision and recall [Chen 09] values for each user is calculated – two standard decision support widely used in information retrieval and, more recently, in recommendation system [Yu 03]. Precision is the ratio of the amount of recommended content in which the user was interested to the amount of content recommended, while recall is the ratio of the amount of recommended content of interest to the amount of content of interest in the collection:

$$\text{Precision} = \frac{\text{Recommended} \cap \text{interested}}{\text{Recommended}} \qquad (9)$$

$$\text{Recall} = \frac{\text{Recommended} \cap \text{Interested}}{\text{Interested}} \qquad (10)$$

As discussed in section 6.2, the recommendation system updates the connection weight values automatically according to user's feedback on the contents in the recommendation list. The more feedback given by the user to the recommendation system, the more accuracy will the system provide. In Figure 6-7, it is noticed that with the increase of content to which the user gives his feedback, the precision and recall increase at first and then the precision values remain stable between 0.88 and 0.91 and the recall values remain stable between 0.81 and 0.84.

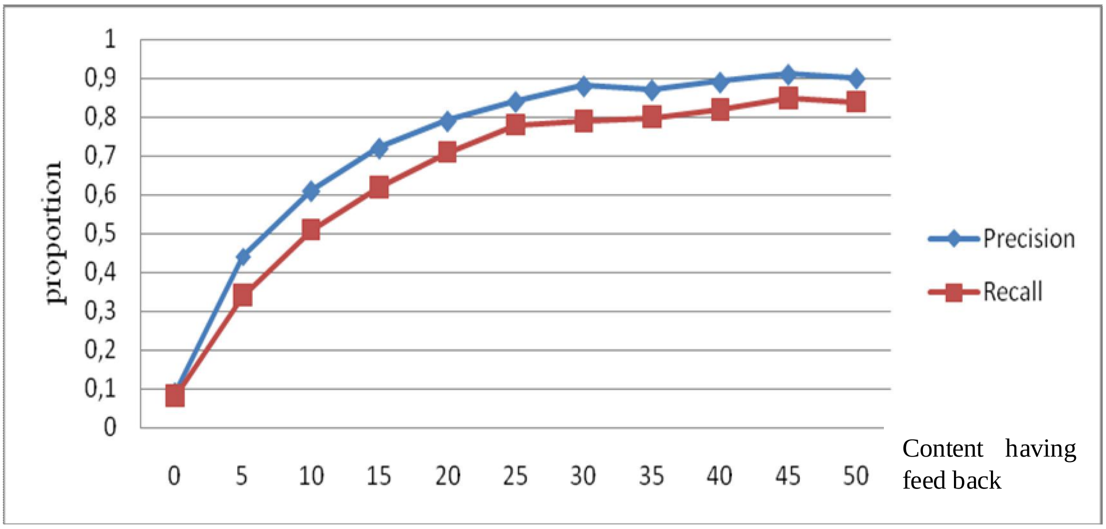


Figure 6-7 Accuracy of the content recommendation system

6.8 Conclusion

This chapter presents a context-aware recommendation system which considers not only the user’s explicit preferences but also his implicit preference through introducing the weight values between nodes along the different layers which associates the user's preference to the context information. Content is recommended to each user as well as each group of users based on user’s preference and the global context information. This makes the recommendation more accurate and personalized. This system is implemented and through the performance evaluation, interesting results are observed in terms of the content recommendation delays as well as the recommendation accuracy. The obtained results are promising in enhancing services personalizing the content overload problem.

Conclusion

Internet Protocol TV (IPTV) broadcasts video and multimedia content in digital format via broadband Internet networks and changes the TV model from traditional broadcast model to a new user-centric model. The change in the users' behaviors from active to passive, the content digitization allowing easier distribution, and the broadband enabled technology have changed the TV experience. IPTV allows TV services to evolve into true converged services, blending aspects of communications, social media, interactivity, and search and discovery in new ways. All these triggers the important of IPTV services personalization and allows opening new markets for network operators, service providers and content providers. Although the rapid advancement in IPTV technology, IPTV service personalization is still in its infancy. This thesis presents solutions aiming to improve IPTV service personalization from three aspects:

1) New Personalized IPTV architecture through integrating a context-awareness system. Through investigating the general IPTV service and IPTV architecture in NGN environment as well as analyzing the different related contributions in Chapter 1, it is observed that context-awareness is promising in monitoring users' environment (including networks and terminals), making users' interaction with the TV dynamic and thus enhancing the service personalization. Consequently, some guidelines are given for realizing the IPTV services personalization through context-awareness. After presenting the context information type and context data structure model for the IPTV services in Chapter 2, Chapter 3 proposes a solution for IPTV services personalization that integrates a context-awareness system in the IPTV/IMS architecture and IPTV/Non-IMS architecture allowing the consideration of different context information related to the user, his devices, the network and the service itself in real-time. The solution is implemented on top of an IPTV platform validating its correct functioning and evaluating its performance for TV Live and Video on Demand (VoD) IPTV service compared to classical IPTV case (with no personalization). Promising results are observed for the proposed solutions in terms of the personalized content selection and service initiation delays as well as the Electronic Program Guide (EPG) browsing time.

2) Personalized users' access. The tight attachment of the subscriber authentication to the user equipment limits the personalization of the services. To solve this problem, a new identification and authentication mechanism using RFID and the Identity Based cryptography (IBC) is proposed in chapter 4, which allows service personalization through authenticating users in a personalized manner during services access. This solution is implemented on top of an emulated Generic Bootstrapping Architecture (GBA) architecture. The authentication delay and resources consumed during the authentication are measured. It is observed that the increase in the number of clients does not influence the request average processing time and the average consumed resources. In Chapter 5, the Open BCMP queuing network is used as a mathematical model to evaluate the performance of the proposed Service Authentication based on IBC (SA-IBC) authentication solution. A clustering algorithm is also proposed to improve the performance of the authentication solution through distributing the servers within the SA-IBC architecture according to the service rate of the system. The derived BCMP model for SA-IBC is implemented under MatLab with and without the proposed clustering algorithms and the performance is evaluated through measuring the service utilization and authentication delay. It is observed that the increase in the number of clients has an impact on the server utilization and authentication delay. Furthermore, it is observed that the Bootstrapping Service Function (BSF) presents a bottleneck in the process of service authentication. The proposed clustering algorithm proved to improve the performance of the system and helps in resolving the bottleneck problem.

3) Context-awareness based content recommendation for IPTV services. Besides the user's preference, the general context information (like device capacity, network states, location, time, user’s activity…etc) also takes an important role for the recommendation service, because the user's preference on IPTV content may be changed with the different context information. Chapter 6 proposes a context-aware recommendation system which considers not only the user’s preferences but also the global context information. The proposed system is implemented and the performance related to the recommendation delay and the accuracy is evaluates. It is observed that for reducing the recommendation delay, an offline phase is required for the recommendation system to treat static (or nearly static) context information. It is also observed that considering the context information, makes the recommendation more accurate and personalized.

Future work

The domain of IPTV service personalization is a broad one and is still observing many progresses. This thesis has investigated several problems that are important for providing a personalized IPTV service and presented several research contributions for these problems.

Some appropriate areas for future work are:

- Aiming for services convergence and the development on an open TV model (not limited to the wall garden managed IPTV model), the proposed context-aware system can be integrated in other TV systems such as Internet TV or mobile TV, allowing users to have personalized access to various contents including the user created contents in a transparent mean to the user.
- Context-awareness is promising in enhancing the IPTV service personalization ranging from users' interactivity and content adaptation. The service personalization mean considered in this thesis is mainly the context-awareness based recommendation. In the future, more service personalization means can be considered, for example 1) the media server could adapt the format of the content dynamically according to the network context information ; 2) the personal content can be transferred from terminal to terminal without interrupting the service according to the change of user's location within the domestic sphere implying solutions for the geo-localization; 3) the context-aware IPTV system could also cooperate with other services (for example presence service or the social networks applications) to provide advanced personalized service.
- It is important to consider studies on the scalability of infrastructure, considering a large volume of simultaneous accesses of users which is typical in the field of IPTV. Consequently, the existing platform for the implemented work of this thesis needs to be enriched through analyzing the performance of the whole system in the presence of multiple end-users and including more performance metrics and more scenarios for the user interaction with the system.
- Within the proposed context-awareness system, a graphic modeling based IPTV Context data structure is defined. During the context transmission and processing for the context information, the XML schema based markup modeling is employed to represent the context information. Ontology is another frequently used context modeling solution, which provides a structural framework for organizing information and allows the system to be integrated with some existing logical reasoning mechanisms. In the future, it is suggested

to redefine the context modeling using ontology and compare the preference between the markup modeling and the ontology modeling.

- The proposed Service Authentication based on IBC (SA-IBC) solution also needs to be implemented on a real service platform replacing the emulated one in the thesis and applying the proposed clustering approach. Performance tests with large number of clients also need to be carried out comparing the SA-IBC solution with the traditional GBA-AKA authentication.

List of Acronyms

AAA	Authentication, Authorization and Accounting
AP	Access Point
B2B	Business to Business
B2B2C	Business to Business to Client
BAN	Body Area Network
BPG	Broadcasting Program Guide
CA	Context Awareness
CC/PP	Composite Capability/Preference Profiles
CDNs	Content Delivery Networks
CoD	Content on Demand
CPI	Capability and Preference Information
DLNA	Digital Living Network Alliance
DVB	Digital Video Broadcasting
DVR	Digital Video Recorder
EPG	Electronic Program Guide
GPS	Global Positioning System
HbbTV	Hybrid Broadcast Broadband TV
HD	High Definition
HNED	Home Network End Device
IPTV	IP TeleVision
IETF	Internet Engineering Task Force
ITV	Interactive TV
LLDP	Link Layer Discovery Protocol
LLTD	Link Layer Topology Discovery
KPI	Key Performance Indicators

MAC	Media Access Control
MHP	Multimedia Home Platform
NFC	Near Field Communication
PVR	Personal video recorder
PIDF	Presence Information Data Format
QoE	Quality of Experience
QoS	Quality of Service
RF	Radio-Frequency
RFC	Request for Comments
RFID	Radio-Frequency Identification
RPID	Rich Presence Extension to PIDF
RSSI	Received Signal Strength Indicator
STB	Set Top Box
TOA	Time of Arrival
UI	User Interface
UML	Unified Modeling Language
UPnP	Universal Plug and Play
VoD	Video on Demand
UAProf	User Agent Profile
UI	User Interface
UPnP	Universal Plug and Play
VoD	Video on Demand
WAP	Wireless Application Protocol

Reference

[3GPP] 3rd Generation Partnership Project (3GPP) www.3gpp.org

[3GPP TS 29.229] 3GPP TS 29.229: "Cx Interface based on Diameter – Protocol details"

[3GPP TS 123 228] 3GPP TS 123 228 " IP Multimedia Subsystem (IMS); Stage 2".

[3GPP TS 133.220] 3GPP TS 133.220: “Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture”.

[3GPP2S] 3GPP2 S.R0086-0: “IMS Security Framework”

[Adomavicius 05] Adomavicius, G.; Tuzhilin, A. (June 2005), "Toward the Next Generation of Recommender Systems: A Survey of the State-of-the-Art and Possible Extensions", IEEE Transactions on Knowledge and Data Engineering

[Albin 01] H. Albin-Amiot, P. Cointe, Y.-G. Gueheneuc, and N. Jussien. Instantiating and detecting design patterns: Putting bits and pieces together. ase, 00:166, 2001.

[Ardissono] L. Ardissono, C. Gena1, P. Torasso, F. Bellifemine,, Personalized Recommendation of TV Programs.

[Arvidsson 08] Arvidsson, F.; Flycht-Eriksson, A.. "Ontologies I" (PDF). Retrieved 26 November 2008.

[Baskett 75] F. Baskett, K. Chandy, R. Muntz, and F. Palacios. Open,closed, and mixed networks of queues with different classes of customers. JACM, 22(2):248-260, 1975.

[Boneh 01] D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing”, Proceedings of CRYPTO ’01, LNCS 2139, pages 213-229, Springer-Verlag, 2001

[Booch 00] Grady Booch, James Rumbaugh, Ivar Jacobson (2000). Le guide de l'utilisateur UML

[Bormans 02] Bormans, J., Hill, K ISO/IEC JTC1/SC29/WG11/N5231 MPEG-21 Overview v5. 2002 http://www.chiariglione.org /mpeg /standards/mpeg-21/mpeg-21.htm.

[Bowen 04] Bowen, J.P. and Filippini-Fantoni, S., Personalization and the Web from a Museum Perspective. In David Bearman and Jennifer Trant (eds.), Museums and the Web 2004:

[Brown 97] Brown, P., Bovey, J., and Chen, X. (1997). Context-aware applications: from the laboratory to the marketplace. IEEE Personal Communications, 4(5):58–64.

[Camarillo 06] Gonzalo Camarillo, Miguel-Angel García-Martín, "The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds" (John Wiley & Sons, 2006

[Chen 00] Chen, G. and Kotz, D. (2000). A survey of context-aware mobile computing research. Technical Report TR2000-381, Dept. of Computer Science, Dartmouth College.

[Chen 09] Chen, Y., Huang, H., Min, Y. Community-based Program Recommendation for the Next Generation Electronic Program Guide, IEEE Transactions on Consumer Electronics, Vol.55, No.2, pp.707-712.

[Cruz 09] Cruz, R.S.; Nunes, M.S.; Menezes, L.; Domingues, J.; SIP Based IPTV Architecture for Heterogeneous Networks, 10th International Conference on telecommunication, 2009

[Dhar 05] Dhar, S., 2005. Introduction to Smart Cards. http://www.rootshell.be/~dhar/downloads/SmartCards-Introduction.pdf

[Digital] Digital Living Network Alliance, http://www.dlna.org/home

[DVB] DVB Digital Vides Broadcast http://www.dvb.org/

[DVB 11] Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems 01-2011

[DVB-IPTV] DVB-IPTV, http://www.dvb.org/technology/standards/ ETSI TS 2006

[ETSI TS 182 027] ETSI TS 182 027 v3.5.1 (2011-02) Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IPTV functions supported by the IMS subsystem

[ETSI TS 182 028] ETSI TS 182 028 v3.5.1 (2011-02) Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN integrated IPTV subsystem Architecture.

[ETSI TS 201 812] ETSI TS 201 812 V1.1.1 "Digital Video Broadcasting (DVB); Multimedia Home Platform (MHP) Specification 1.0.3"

[Harbitter 02]Alan Harbitter, Daniel A.Menasee. A Methodology for Analyzing the Performance of Authentication Protocols. ACM Transactions on Information and System Security, Vol. 5, No. 4, November 2002. pp: 458-491.

[Huang 07] C. Huang and J. Li, “One-Pass Authentication and Key Agreement Procedure in IP Multimedia Subsystem for UMTS”, Advanced Information Networking and Applications, AINA, page(s): 482-489,2007

[Hudson 03] Hudson, D. L., Cohen, M. E., 2003. Neural Networks & Artificial Intelligence for Biomedical Engineering, Prentice Hall of India

[Hull 97] HULL R, NEAVES P, and BEDFORD-ROBERTS J. (1997): Towards Situated Computing. In: 1st International Symposium on Wearable Computer, pp 146-153

[IEEE 802.1] IEEE 802.1AB Standard, Station and Media Access Control Connectivity Discovery http://standards.ieee.org/getieee802/download/802.1AB-2005.pdf

[IETF] IETF Internet Engineering Task Force http://www.ietf.org/

[ITU 08] ITU-T IPTV Focus Group Proceeding 2008

[ITU-T] ITU-T: International Telecommunication Union – Telecommunication http://www.itu.int/ITU-T

[Kiss 07] Kiss, C. Composite capability/preference profiles (CC/PP): Structure and vocabularies 2.0 April 2007 http://www.w3.org/TR/2007/WD-CCPP-struct-vocab2-20070430/

[Klyne 04] Klyne, G., Carroll, JJ., McBride, B., Resource description framework (RDF): Concepts and abstract syntax. 2004. http://www.w3.org/TR/rdf-concepts/

[Landt 01] Landt, Jerry (2001). "Shrouds of Time: The history of RFID"

[Leon-Garcia 08] Alberto Leon-Garcia (2008). Probability, statistics, and random processes for electrical engineering (3rd ed.). Prentice Hall

[Levine 92] Levine, John R; Mason, Tony; Brown, Doug (1992). LEX & YACC (2 ed.). O'Reilly. pp. 1–2. ISBN 1-56592-000-7.

[Link] Link Layer Topology Discovery Protocol Specification, http://msdn.microsoft.com/en-us/windows/hardware/gg463024

[Liu 08] Wei Liu, Lin Yang, Quan-Lin Li, Hao Dai, Bin Hou: Performance Analytic Model for Authentication Mechanism. ICNSC 2008.

[Lonnfors 08] Lonnfors, M., Kiss, K. 2008 Session Initiation Protocol (SIP) User Agent Capability Extension to Presence Information Data Format (PIDF). http://www.ietf.org/rfc/rfc5196.txt

[Martinez 04] Martinez J.M. ISO/IECJTC1/SC29/WG11 N6828 MPEG-7 Overview 2004. http://www.chiariglione.org/mpeg/ standards/mpeg-7/mpeg-7.htm.

[Matlab] Matlab http://www.mathworks.com/products/matlab/

[Miracl] Miracl: “Multiprecision Integer and Rational Arithmetic C/C++ Library”, available in http://www.shamus.i

[Moon 06] Moon, A., Kim, Hs.., Lee, K., Kim, H. 2006 Designing CAMUS based Context-Awareness for Pervasive Home Environments. International Conference on Hybrid Information Technology, pp. 666--672, Cheju Island

[MPEG] MPEG http://www.chiariglione.org/mpeg/

[Open] Open IPTV Forum, http://www.openiptvforum.org

[Priselac 08] D. Priselac, M. Mikuc, “Security risks of pre-IMS AKA access security solutions”, available in http://www.ericsson.com/hr/etk/dogadjanja/mipro_2008/1227.pdf

[Rascioni 09] Rascioni, G., Spinsante, S., Gambi, E. 2009 Non Conditional Smart Card Technology to Deliver Personalized iTV Services. Proceedings EuroITV 2009 Networked Television, Leuven, Belgium

[RFC 3310] RFC 3310, “Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)”, 2002.

[Ring 06] J. Ring, K. Raymond Choo and E. Foo, “A New Authentication Mechanism and Key Agreement Protocol for SIP Using Identity-based Cryptography”, AusCERT2006 R&D Stream. Gold Coast, Australia, 2006.

[Rosenberg 02] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, H., Schooler, E. SIP: Session Initiation Protocol 2002 http://www.ietf.org/rfc/rfc3261.txt

[Rosenberg 04] Rosenberg, J., Schulzrinne, H., Kyzivat, P., Indicating User Agent Capabilities in the Session Initiation Protocol (SIP) 2004. http://www.rfc-editor.org/rfc/rfc3840.txt

[Ruby] Ruby, Sam; Thomas, Dave; Hansson, David (March 28, 2009). Agile Web Development with Rails.

[Santos 01] Santos, J.B.D., Goularte, R., Faria, G.B., Moreira, E.D.S. 2001 Modeling of user interaction in context-aware interactive television application on distributed environments, 1st Workshop on Personalization in Future TV, Sonthofen

[Santos 09] Santos da Silva, F., Alves, LGP., Bressan, G.2009 PersonalTVware: A Proposal of Architecture to Support the Context-aware Personalized Recommendation of TV Programs. Proceedings EuroITV 2009 Networked Television, Leuven, Belgium

[Schilit 94] B. Schilit, N. Adams, and R. Want. (1994). "Context-aware computing applications" (PDF). IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'94), Santa Cruz, CA, US. pp. 89–101.

[Schulzrinne 03] H. Schulzrinne, S. Casner, R.Frederick, V.Jacobson.: RTP: A Transport Protocol for Real-Time Applications. In: IETF RFC 3550 (2003)

[Schulzrinne 06] Schulzrinne, H., Gurbani, V., Kyzivat, P., Rosenberg, J. RPID Rich Presence Extensions to the Presence Information Data Format (RPID) 2006. http://tools.ietf.org/html/rfc4480

[Shamir 84] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes" 1984.

[Sher 06] M. Sher, T. Magedanz: Secure access to IP multimedia services using generic bootstrapping architecture (GBA) for 3G & beyond mobile networks. Q2SWinet 2006: 17-24

[Song 11] S. Song, M. Abid,H. Moustafa, A. Afifi, " Performance Evaluation of an Authentication Solution for IMS Services Access", telecommunication systems journal, 2011

[Steele] TJ. Michael Steele, "The Cauchy-Schwarz Master Class: An Introduction to the Art of Mathematical Inequalities"

[Strong] Tomas Strong and Claudia Linnhoff-Popien A Context Modeling Survey

[Sugano 04] Sugano, H., Fujimoto,S., Klyne, G., Bateman, A., Carr, W., Peterson, J., Presence Information Data Format (PIDF) 2004 http://tools.ietf.org/html/rfc3863

[Thawani 04] Thawani, A., Gopalan, S. 2004. Sridhar, V.: Context Aware Personalized Ad Insertion in an Interactive TV Environment. 4th Workshop on Personalization in Future TV

[Thomas 93] Gruber, Thomas R. (June 1993). "A translation approach to portable ontology specifications". Knowledge Acquisition 5 (2): 199–220.

[TISPAN] TISPAN: Telecoms & Internet converged Services & Protocols for Advanced Networks, http://www.etsi.org/tispan/

[TV-Anytime] TV-Anytime http://tv-anytime. org/

[Universal] Universal Plug and Play, http://www.upnp.org/

[W3C] W3C World Wide Web Consortium: http://www.w3.org

[WAG] WAG User Agent Profile 2001 http://www.openmobilealliance.org/tech/affiliates/wap/wap-248-uaprof-20011020-a.pdf

[WAP] WAP Forum Wireless Application Protocol Forum: http://www.wapforum.org/what/technical.htm

[Weiser 91] Weiser, M. (1991). The computer for the 21st century. Scientific American, 265(3):66–75.

[Wu 09] L. Wu, Y. Zhangb and F. Wang, “A new provably secure authentication and key agreement protocol for SIP using ECC”, Computer Standards & Interfaces Volume 31, Issue 2, Pages 286-291, February 2009

[X9.62] ANSI. X9.62. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). 1999.

[Xiao 07] Y. Xiao, X. Du, J. Zhang, F. Hu, and S. Guizani, “Internet Protocol Television (IPTV): The killer application for the next-generation internet,” IEEE Communications Magazine, vol. 45, no. 11, pp. 126–134, Nov. 2007.

[XMLTV] XMLTV http://xmltv.myftp.org/

[Yu 03] Zhi-wen YU, Xing-she ZHOU, Jianhua GU, Xiaohun WU, ADAPTIVE PROGRAM FILTERING UNDER VECTOR SPACE MODEL AND RELEVANCE FEEDBACK Proceedings of the Second International Conference on Machine Learning and Cybernetics, Xi’an, 2-5 November 2003

Publications

Journals

[1] M. Abid, S. Song, H. Moustafa, H. Afifi, "Integrating Identity-Based Cryptography in IMS Service Authentication," International Journal of Network Security and Its Applications (IJNSA), Volume 1. Number 3, pages: 1- 13, October 2009

[2] S. Song, M. Abid, H. Moustafa, H. Afifi, "Performance Evaluation of an Authentication Solution for IMS Services Access," accepted for the special issue "wireless and network security" in Telecommunication Systems journal- To appear

[3] S. Song, H. Moustafa, H. Afifi, "A Survey on Personalized TV & NGN Services through Context-Awareness," accepted for publication in ACM Computing Surveys-To appear

[4] S. Song, H. Moustafa, H. Afifi, "IPTV Services Personalization using contextAwareness", accepted for the International Journal of Informatica, SI on IPTV and Multimedia services-To appear

[5] S. Song, H. Moustafa, H. Afifi, "Advanced IPTV Services Personalization through Context-Aware Content Recommendation," submitted to IEEE Transaction on Multimedia – SI on smart, social and converged TV.

Conferences

[1] S. Song, H. Moustafa, H. Afifi, "Context-Aware IPTV," IFIP/IEEE Management of Multimedia & Mobile Network Service (MMNS 2009)

[2] M. Abid, S. Song, H. Moustafa, A. Afifi, "Efficient Identity-Based Authentication for IMS based Services Access," ACM Mobile Computing & Multimedia 2009 (MOMM 2009)

[3] S. Song, H. Moustafa, H. Afifi, "Personalized TV Service through Employing Context-Awareness in IPTV/IMS Architecture," International Workshop on FUTURE MULTIMEDIA NETWORKING (FMN 2010)

[4] S. Song, H. Moustafa, H. Afifi, "Modeling an NGN authentication solution and improving its performance through clustering," submitted to IEEE International Conference on Communications (ICC2012) -- Submitted

[5] S. Song, H. Moustafa, H. Afifi, "Enriched IPTV services Personalization" submitted to IEEE International Conference on Communications (ICC2012) -- Submitted

Patents

French Patent, INPI # 1060396 "Gestion de Service IPTV dans un Réseau", S. Song & H. Moustafa, December 2010.

French Patent, INPI # 1052348 "Gestion de Service IPTV/IMS dans un Réseau", S. Song & H.Moustafa, March 2010.

French Patent INPI # 1159503 “Services de recommendation pour IPTV se basant sur context-awareness" S. Song & H. Moustafa