An Access Control Framework of Federated IPTV Providers for Mobile IPTV Services

María Elizabeth Aldana Díaz and Eui-Nam Huh

Department of Computer Engineering, Kyung Hee University,
Global Campus, South Korea
{maeliz,johnhuh}@khu.ac.kr

Abstract. M-IPTV service provision depends on different administrative domains to deliver individualized service and timely/on-demand and forces service providers to use effective mechanisms and strategies of resource management in order for them to be able to guarantee the quality levels their customers' demands during service provisioning. This paper, proposes a protocol for secure M-IPTV service provision delegation to support IPTV provider' SLAs through access control extension to different IPTV provider' security domains using Single Sign-On (SSO) technique along with handling individualized policies helping to improve communication and collaboration in B2B environment and providing users with a more consistent unified experience and seamless logon.

Keywords: Mobile IPTV, Service Level Agreements, Access control, Single Sign-on, SAML.

1 Introduction

IPTV dependencies of success have been analyzed from consumer and supplier perspective [1]. Truly interactive experience, attractive service, content-driven platform and availability of the technology to actually utilize all that it offers will guarantee IPTV success from consumer point of view. Accordingly, the ability to personalize content also gives the various service providers the ability to gather all sorts of information regarding a consumer's particular preferences increasing their use of more personalized targeted advertising, with a potentially higher chance of instigating sales.

Shin [19] study shows the user factors driving the adoption of IPTV and classifies them in intrinsic factors i.e. seeking high quality, content-rich, and value added services; and extrinsic factors i.e. highly interactive services and interoperable applications with other devices and platforms. Taking all the variables into account, the results of logistic regression shows that quality of content (special individualized service and timely/on-demand) and interactive services (value-added service and compatibility) are indeed significant predicators of the diffusion of IPTV.

IPTV services are originally targeted to fixed terminals such as set-top boxes used by different users; however, issues on the requirements for mobility support

T.-h. Kim et al. (Eds.): FGIT 2010, LNCS 6485, pp. 413–428, 2010.

were raised as an out-growth under the auspices of the Fixed-Mobile Convergence (FMC) trend. Therefore, new personalized IPTV targets have came up to expand its value such as Mobile IPTV (M-IPTV) that enables users to transmit and receive multimedia traffic including television signal, video, audio, text and graphic services through IP-based the wired and wireless networks with support for QoS/QoE, security, mobility, and interactive functions. Through Mobile IPTV, users can enjoy IPTV services anywhere and even while on the move. There are four M-IPTV approaches which have been developed [18]: Mobile TV plus IP, IPTV plus Mobile, Cellular and Internet. Mobile TV plus IP is a convergence service between broadcasting, telecommunications and computing. IPTV plus Mobile is dominated by Telco giants in an attempt to find a new source of cash-in. Cellular is represented by Open Mobile Alliance [4] initiative defining end-to-end framework for mobile broadcast. At last, Internet approach known as Internet TV or Web TV has a short coming: that the quality of services is not guaranteed. However, considering its rapid adaptation to customer needs, this approach may be dominant in the near future. As long as mobile device uses Internet, users can access to IPTV service through various wireless access networks.

In multimedia services, security and privacy issues are urgent to be solved, such as content security and service protection. To solve these issues, some means have been proposed, such as conditional access and digital rights management. Lian's [11] work provide a digital rights management scheme for the convergent services through scalable encryption and transcoding, various business models and encryption modes and adaptive decryption.

M-IPTV service provision depends on different administrative domains to deliver individualized service and timely/on-demand and forces service providers to use effective mechanisms and strategies of resource management in order for them to be able to guarantee the quality levels their customers' demands during service provisioning. Service level agreements (SLA) are the most common mechanism used to establish agreements on the quality of a service (QoS) between a service provider and a service consumer. From the user's point of view, he expects to watch a TV program related to his preferences over his mobile phone. From IPTV provider, he makes sure the requested content is available before authorize the service, if is not, asks other IPTV provider who has same content to deliver it in order to avoid SLA violations. The key challenge for this scenario is SLAs adaptation, when IPTV provider lacks of capabilities and resources to deliver the agreed service sends consumer's SLA profile including user's policy related attributes to other IPTV provider delegating service provision to other providers efficiently. To authenticate the user Single Sign-On (SSO) [9] is a good way to access other systems. SSO is an access control of multiple, related, but independent software systems. With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them.

Therefore in this work we propose to support IPTV provider's SLA through access control extension to different IPTV provider's security domains using Single sign-on technique along with handling individualized policies.

This paper is organized as follows. Section 2 provides a detailed state of the art overview of M-IPTV authentication methods, SSO approaches and SLA's implementation scenarios. In Section 3, we introduce the M-IPTV framework and secure service protocol. The performance evaluation is analyzed in Section 4. Finally, conclusions are presented in Section 5.

2 Related Work

2.1 M-IPTV Access Control

M-IPTV access control is a process by which the use of mobile multimedia resources is regulated according to a security policy and the result is a set of authorized interactions a subscriber can do with it.

Till now, efficient service protection protocols regarding IPTV by means of mobile devices have been proposed, which can be classified in three types: Data Rights Management (DRM) [11,13], IP CAS [7] and subscriber authentication technologies in AAA mechanism [17]. DRM is a technology adopted to control rights of digital content that uses Conditional Access System (CAS) [4]. CAS comprises a combination of scrambling and encryption to prevent unauthorized reception. Scrambling is the process of rendering the sound, pictures and data unintelligible. Encryption is the process of protecting the secret keys that have to be transmitted with the scrambled signal in order for the descrambler to work. Entitlement Control Messages (ECMs) are combined with a service key and the result is decrypted to produce a control word that is periodically updated. Entitlement Management Messages (EMMs) are sent over-air encrypted with a unique Master Key, pre-shared in subscriber's receiver, and carries entitlement information that includes service key and expiration date for each valid subscriber. IP CAS is a technical transplantation from broadcasting cable network to IP network with negative implications in quality and service. In quality, IP packets stream suffers a lot from disorder, delay, and jitter. In service, IP network carries different types of digital service that decrease the performance. Specialized physical client security module make CAS unsuitable for M-IPTV. Different from CAS, subscriber authentication technologies in AAA mechanism utilizes for subscriber authentication, counter-based OTP and Admissible Bilinear MAP based authorization ticket method, and even when the service channel is changed from home network to foreign network, the mobile IPTV services are consistently provided by means of authorization tickets.

2.2 Single Sign-On

The basic idea of single sign-on (SSO) is access control of multiple, related, but independent software systems. With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them. The SSO service acts as the wrapper around the existing security infrastructure that exports various security features like authentication and authorization.

Different approaches for Web SSO implementation have been proposed XML-Based [8,9], One Time Password [20] and Kerberos [5,6]. XML-Based approach, provide flexibility, extensibility, and interoperability between environments to be integrated and also user authentication and access control using Security Assertion Markup Language (SAML) [15,16], a standard specification which is ratified by Organization for Advancement of Structure Information Standard (OASIS) [14]. One Time Password, it entails the user to use different password for each login to establish the communication among the applications. It eliminates the necessity of setting up the new infrastructure and also the existing system requires minimal changes to incorporate the single sign-on feature in it. It does not expose user's static and long lived password directly in the network. Kerberos SSO implementation offers the ability to prove their authenticity once in a period, and to cache the fact that authentication was successful so that subsequent authentications conducted by client software on behalf of the user need not involve the user. However, access control policies may impose other requirements that could cause users to have to re-authenticate, or provide additional proofs of authenticity. Enterprise SSO makes Kerberos credentials delegation quite difficult. However, Kerberos deployments commonly only use shared secret authentication, the protocol does support other methods of authentication and the use of Kerberos can significantly degrade a Web application's performance.

XML-Based combine with SAML has advantage over Web SSO solutions since it is a standard suitable for facilitating site access among trusted security domains after single authentication. SAML provides distributed authorization and federated identity management, and does not impose a centralized, decentralized, or federated infrastructure or solution, but instead facilitates the communication of authentication, authorization, and attribute information.

2.3 Service Level Agreement

Service level agreements (SLA) are the most common mechanism used to establish agreements on the quality of a service (QoS) between a service provider and a service consumer. SLANg [10] is a SLA specification based on XML language which integrates non-functional features (service levels) of contracts between independent parties with the functional design of a distributed component system for service provisioning horizontally or vertically. Horizontal SLAs govern the interaction between different parties providing the same kind of service whereas Vertical SLAs regulate the support parties get from their underlying infrastructure, within the service provision. SLANg defines seven different types of SLA based on a service reference model, i.e. Application, Web Service, Component, Container, Storage and Network.

Application SLAs approach is proposed in [12] as a middleware architecture for enabling Service Level Agreement (SLA)-driven clustering of QoS-aware application servers. It dynamically supports application server technologies with dynamic resource management to meet application-level QoS requirements. These requirements include timeliness, availability, and high throughput and are specified in SLAs. The middleware architecture incorporates three principal

QoS-aware middleware services: a Configuration Service, a Monitoring Service, and a Load Balancing Service to balance client requests among clustered servers, based on the actual load of those servers, thus preventing server overloading. The size of the cluster can change at runtime, in order to meet nonfunctional application requirements specified within hosting SLA. Web Service SLA [3] is intended for an enterprise server (or cluster) working as a web services provider, which supplies a collection of services through Internet to servers of other enterprises. The operational environment defines C2B connections between end clients and consumer servers, and B2B relationships between consumer servers and provider servers. Therefore, when the current load supported by the cluster is below the maximum admissible load determined from the SLA, the QoS control mechanism does not reject any new session requests. This study demonstrates that the QoS control mechanism carries out an effective differentiation of the service provided to consumers, reserving the processing capacity of the cluster for the preferential consumers during the overload periods. Moreover, the QoS control mechanism does not produce over reservation of processing capacity for the preferential consumers when the cluster operates under normal load conditions. This mechanism considers classes of requests and categories of consumers; it also guarantees the SLAs during overloads, giving priority to the service of preferential consumers.

Dynamic Networking SLAs [2] can take place between User and a Network Provider Agent which enables dynamic and flexible bandwidth reservation schemes on a per-user or per application basis. This architecture facilitates quantitative bandwidth, session duration, session start time, preferences, negotiations per user or per flow basis via SLA. The results show that these schemes can be exploited for the benefits of both negotiating parties such as getting the highest individual SLA optimization in terms of QoS and price. It is shown that in most cases, negotiation reduces rejection probability.

The fact that different types of service's SLAs are determined in XML language makes it easily extensible to increase expressiveness of non-functional features of contracts between independent parties with the functional design of a distributed component system for service provisioning.

3 Proposal

3.1 M-IPTV Framework

We design a framework based on M-IPTV service provision where mobile subscriber expects to watch a TV program related to his preferences over his mobile phone. IPTV provider makes sure the requested content is available before authorize the service, if is not, asks other IPTV provider who has same content to deliver it in order to avoid SLA violations. The key challenge for this scenario is SLAs adaptation, when IPTV provider lacks of capabilities and resources to deliver the agreed service sends consumer's SLA profile to other IPTV provider delegating service provision.

Following the above-described scenario, this framework represents an identity federation where users coming from the home IPTV provider access protected resources offered by another IPTV provider belonging to the same federation. IPTV providers belonging to identity federation demand a finer user access control in order to offer value-added services: in this case, special individualized service and timely/on-demand. M-IPTV federation scenario focuses on the protection of high-level services offering authentication mechanisms for end users, based on login/password which can be enhanced using SSO to access federation resources without further re-authentication. Another characteristic in the federation deployed is the use of access control mechanisms based on the user information i.e. age, gender and SLA which are defined in their home IPTV provider and are called user attributes.

This framework is a novelty solution which offers access control architecture to protected resources inside federation and provides mechanisms to manage both user authentication and authorization. The former is based on traditional methods and the latter on the use of authorization management techniques, making use of the user attributes, defined in their home IPTV provider to extend the federation allowing differentiated services provision to end users. SSO mechanism uses a token obtained during access, and then can be used to gain access to other services offered by the IPTV providers belonging to the federation. Figure 1 shows M-IPTV framework. The participant entities are Subscriber, Mobile Communication Network and IPTV provider federation.

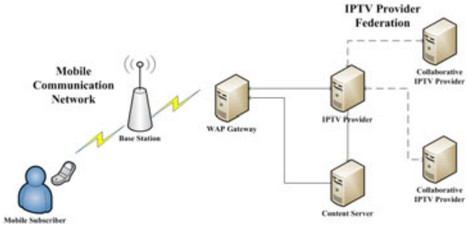

Fig. 1. M-IPTV framework

To provide access control based on user attributes, it is necessary to introduce the following features: first, IPTV providers need to define which user attributes (type and value) they are going to be responsible for that task (SLA), second, we have to define the protocol to service provision delegation. We can transport those requests through the same channel used to exchange authentication requests. Moreover, in order to provide a generic and extensible authorization environment, it would be desirable to make use of a generic framework able to hide the implementation details of the different identity management solutions deployed by each IPTV provider.

In order to provide SSO functionalities we need to cover the following issues: some kind of token needs to be defined in order to provide services with a way to be aware of the users who have been successfully authenticated and for whom no new authentication process is required. Also, the token is user transparent where the SSO process should be managed by the federation components themselves.

The following sections describe the different underlying components of the proposed framework.

3.2 Security Assertion Markup Language

SAML [15] is an XML-based framework for communicating user authentication, entitlement, and attribute information. It allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application. SAML's components [16] are:

Assertions: SAML allows for one party to assert security information in the form of statements about a subject. It contains some basic required and optional information that applies to all its statements, and usually contains a subject of the assertion (if not present, the identity determined through other means, e.g. the certificate used for subject confirmation), conditions used to validate the assertion, and assertion statements. SAML defines three kinds of statements that can be carried within an assertion: authentication, these are created by the party that successfully authenticated a user describing the particular means used to authenticate the user and the specific time at which the authentication took place; attribute, these contain specific identifying attributes about the subject; and authorization decision, these define something that the subject is entitled to do.

Bindings: SAML bindings detail exactly how the various SAML protocol messages can be carried over underlying transport protocols.

Protocols: SAML defines a number of request/response protocols that allow service providers to authenticate a principal or get assertions that meet particular criteria e.g. Artifact Resolution Protocol which provides a mechanism by which SAML protocol messages may be passed by reference using a small, fixed-length value called an artifact using one SAML binding (e.g. HTTP Redirect) while the resolution request and response take place over a synchronous binding, such as SOAP.

Profiles: Generally, a profile of SAML defines constraints and/or extensions in support of the usage of SAML for a particular application, the goal being to enhance interoperability by removing some of the flexibility inevitable in a general-use standard.

3.3 Architecture

The architecture, as shown in Figure 2, is based on secure service convergence scheme composed of User, Distribution Networks and Content Provider [11]. Among them, User sends M-IPTV service request using his mobile phone. The service request is transmitted over Mobile Communication Networks who acts as Distributor Network through WAP Gateway which connects the mobile domain and the wired Internet acting as protocol gateway to encode and decode from WAP-HTTP and vice versa respectively. IPTV provider authenticates and authorizes mobile subscriber request. If authorization process is successful Content Provider processes the multimedia content, including encoding, encryption, packaging and right issuing. Mobile Phone decrypts and descrambles content and mobile subscriber plays securely the content.

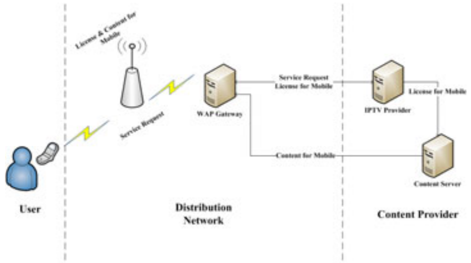

Fig. 2. Architecture of M-IPTV secure service

We propose M-IPTV architecture for secure service delegation which supports SLA adaptation. Figure 3 shows the concept of this architecture. IPTV provider receives service request, he authenticates mobile user and makes sure he counts on all resources to deliver the agreed service i.e. the requested content is available, before authorize the service. If he cannot deliver the agreed service negotiates with other IPTV provider to provide service. The negotiation is based on SSO and access control using SAML which is standardized specifications to provide flexibility, extensibility, and interoperability between environments to be integrated.

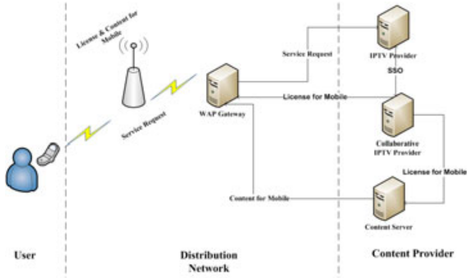

Fig. 3. M-IPTV architecture for secure service delegation

3.4 M-IPTV Secure Service Delegation Protocol

When a customer wants to use a service offered by an IPTV provider, an agreement is needed, in the same way of a traditional service. The contract involves both functional and not functional parameters relating to the service to be provided. SLA is the most common mechanism used to establish agreements on the QoS between a service provider and a service consumer.

The M-IPTV interaction process is shown in Figure 4. Firstly, the user requests to the IPTV Provider for the service. Secondly, IPTV provider authenticates the user, checks SLA to authorize the service and sends the License to the user. Thirdly, the Content Server sends content for Mobile.

The higher the number of service requests needed to be served, the higher the probability that task is not accomplished because of inability of IPTV provider to meet an SLA's objectives and the provision of a service to the customer is not successfully carried out. In such rigid context, the QoS of the final service can be strongly affected by violation on user's SLA. In order to prevent such violations SLA need to adapt during service provision with a flexible mechanism enabling the run-time negotiation of the guarantees on the QoS with other IPTV providers once violations on such guarantees are expected to occur. This would avoid both the suspension of the service provisioning and the brutal termination of the agreement.

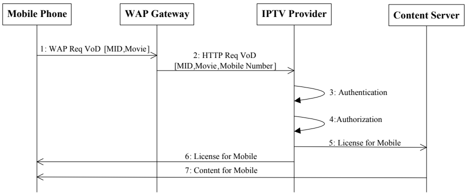

Fig. 4. M-IPTV service delivery protocol

The flexibility that we refer to consists in the possibility of (1) negotiating at run-time the service provision with SLA guarantees with others IPTV providers, and (2) accordingly delegate service delivery. This process, of course, must preserve the continuity of the service provision, i.e. the service flow must not be either interrupted or suspended while the service delegation is being negotiated.

The protocol being designed must take into account the dynamics and the new requirements that the scenario presented in this section impose. We remark that in such scenario there are several actors, in the role of IPTV provider, that stipulate one-to-one agreements with each others. We must consider:

- Mobile subscriber authentication
- M-IPTV authorization based on SLA profile
- Service delegation

Focusing on the just described requirements, in this work we add the functionality that enable the parties involved in a scenario of service delegation to negotiate SLAs guarantees while service is being provided. Figure 5 shows the concept of the proposed negotiation protocol. Firstly, the user requests to the IPTV Provider for the service. Secondly, IPTV provider authenticates the user, checks SLA to authorize the service and predicts that it does not have enough resources to deliver SLA's. Thirdly, IPTV provider redirects service request to other IPTV provider. To provide flexibility, extensibility, and interoperability between environments to be integrated, SSO based on SAML provides seamless user access to both home and collaborative IPTV security domain. IPTV collaborative provider requests a SAML authentication statement from primary IPTV provider and then, based on the authentication assertion requests an SAML attributes assertion to facilitate the SLA's terms and guarantees exchange. The terms represent contractual obligations and include a description of the service as well as the specific guarantees given that IPTV provider should assure by the availability of resources and/or on service qualities. Fourthly, collaborative IPTV provider checks SLA profile and is called to accept or reject it. If it accepts the proposal, IPTV provider will delegate service delivery; if the proposal is rejected, IPTV provider will continue asking other IPTV providers to provide M-IPTV service.

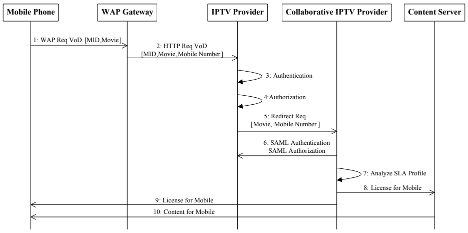

Fig. 5. M-IPTV secure service delegation protocol

Furthermore, IPTV provider might not need to access the service offered by collaborative IPTV provider anymore (unless that service is useful to satisfy other pending requests).

4 Performance Evaluation

The proposed protocol is analyzed according to M-IPTV access control requirements and Service Level Agreement.

4.1 M-IPTV Access Control Analysis

In this section we describe and analyze the M-IPTV access control requirements. Table 1 presents the analysis result.

- Mobile user: User who can transmits and receives multimedia traffic including television signal, video, audio, text and graphic services through IP-based wireless networks with support for QoS/QoE, security, mobility, and interactive functions. The proposed architecture scheme focuses on M-IPTV service provision.

- Cross-domain authentication: Secure process which confirms user's identity with a specified level of confidence. The proposed protocol uses SSO strategy to help improve communication and collaboration in B2B environment and provides users with a more consistent unified experience and seamless logon. After successful authentication and authorization from the main logon, should be able to access external IPTV providers.
- Encryption level: It is necessary to classify the authority over access such as playing multimedia content so as to prevent any unapproved access attempt. In our design, we encrypt the NAL header only instead of doing all contents to avoid tremendous overhead on mobile devices, while DRM is not suitable for mobile devices. The detail of the mechanism is out of scope in this research.
- Multiple attributes authorization: Any information used for access control purposes. The security information described by SAML is expressed in XML format for assertions which are a declaration of a certain fact about an entity i.e. user and device. For the user, the attributes are age, gender, payment information, SLA profile, and file access permissions such as read, write and delete. Regarding the device, the attributes are type of terminal and special features.
- SLA: Service level agreements (SLA) are the most common mechanism used to establish agreements on the quality of a service (QoS) between a service provider and a service consumer. IPTV provider authorizes M-IPTV service based on SLA profile analysis to make sure it has enough resources to deliver service. If IPTV provider is unable to meet an SLA's objectives to provide service asks other IPTV provider who has same content to deliver it in order to avoid SLA violations.
- Secure service delegation: When a service request is redirected to other security domain, it considers the maintenance of privacy and identity control. IPTV provider can securely redirect M-IPTV service request in order to provide service with SLA using SSO mechanism based on SAML to provide seamless user access to both primary and collaborative IPTV security domain. Collaborative IPTV provider requests a SAML authentication statement from primary IPTV provider and then, based on the authentication assertion requests an SAML attributes assertion to facilitate the SLA's terms and guarantees exchange. Collaborative IPTV provider checks SLA profile and decides to accept or reject service provision.

4.2 Service Level Agreement

SLA adaptation process is evaluated by means of the SLA level indicator. From IPTV provider's perspective, the SLA adaptation is satisfactory if SLA's level is fair independently of the quantity of content requested. This outcome is fair if IPTV provider manages to negotiate and delegate service provision to other IPTV providers. From the customer's perspective, SLA adaptation is satisfactory if the probability that its requests are rejected or accepted with SLA violations is low and accepted requests have a high quality.

Table 1. Analysis of proposed scheme

	DRM	CAS	Proposed scheme
Mobile User	no	yes	yes
Cross-domain authentication	no	no	yes
Encryption level	heavy	heavy	light
Multiple attributes authorization	no	no	yes
SLA	not related	not related	yes
Secure service Delegation	no	no	yes

Therefore, to evaluate the satisfaction of customers and IPTV provider, the average SLA of accepted requests clearly represent fundamental performance parameters to be measured. In our model, requests increase at an average rate of three requests per second.

We compare the SLA adaptation scenario with a reference scenario without adaptation, where the IPTV provider maintains SLA's level by itself. The reference scenario represents current practice, where as providers SLA decreases and service provision stops to avoid SLA's violations. The adaptation and reference scenarios are described respectively. Figure 6 shows both scenarios where SLA's level is fair between 6 and 7 level.

SLA adaptation scenario. As discussed in Section 3, the behavior of the IPTV provider is characterized by the negotiation attitude towards collaborative IPTV providers which can be more efficient providing service depending on its available capacity and resources. The behavior of a collaborative IPTV provider is characterized by authorize or not service delegation. The negotiation is comprised of external access control and policies related multi-attributes authorization. Collaborative IPTV provider accepts service delegation and SLA's service level objectives are met to successfully carry out the provision of the service.

Reference scenario without adaptation. In the reference scenario, the mobile subscriber population places service requests at an average rate and IPTV provider verifies whether it has enough capabilities to guarantee SLA. If the capabilities are sufficient, the service request is accepted otherwise, is rejected, no adaptation is performed.

Generally, the SLA adaptation scenario exhibits a better performance than the reference scenario. In particular with higher rate of requests, that is, when capacity becomes a scarce resource, SLA is considerable fair or stable. Without adaptation, allocated capacity grows as average rate increases until saturates. The adaptation mechanism delays saturation, as capacity is allocated only to requests judged worthy by authorization process. Adaptation filters non-satisfactory capacity allocation requests only to delegate service provision fulfilling negotiation criteria. In turn, this increases the rate of accepted requests preserving the continuity of M-IPTV service provision. Otherwise, reference scenario shows that SLA

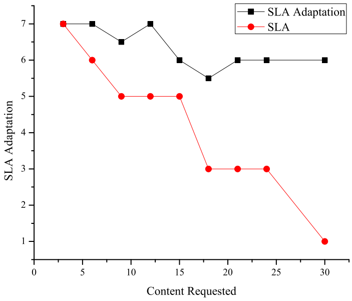

Fig. 6. Service Level Agreement scenarios

decreases proportionally to the quantity of services provided causing suspension of the service provisioning and the brutal termination of the agreement.

Adaptation provides a gain for both IPTV provider and the collaborative IPTV provider for content requested as their SLA level indicator is lower in the reference scenario. A cooperative behavior of collaborative IPTV provider allocates capacity to service requests, with positive effects when capacity is a scarce resource.

Analyzing SLA Adaptation scenario, the delivery percentage of content requested that IPTV provider has allocated at time t=1,2,3..10 at an average rate of three requests per second, ranges from 0 to 100 percentage and decreases when a new request is accepted through SLA adaptation, while it increases when a previously accepted request terminates and the associated capacity is released and used for another request. Figure 7 shows this dynamic process. In this case, 10 scenarios are presented where collaborative IPTV provider offers the same service and the same guarantees as those offered by IPTV provider. Sometimes IPTV provider might not need to access the service offered by collaborative IPTV provider, such is the case of scenario 1 where IPTV provider has enough capacity to manage 100 percentage of the content requested but when is unable to provide M-IPTV service delegates service provision to collaborative IPTV Provider and only manages 18 percentage of the content requested comparing to 88 percentage that collaborative IPTV provider manages in scenario 9.

SSO Efficiency. In the previous section we have analyzed the performance of our protocol and we have compared it with a reference scenario without adaptation. In order to complete our analysis, in this section we compare the efficiency of our access control technique based on SSO to multiple logon in case of rejection. SSO is a main component of the proposed protocol extending access control to different collaborative IPTV provider security domain without being prompted to log in again at each one of them.

SSO aims to simplify the authentication procedure. In this case, when service provision is delegated the user is not re-authenticated instead of it collaborative IPTV Provider pulls authentication and authorization information to analyze

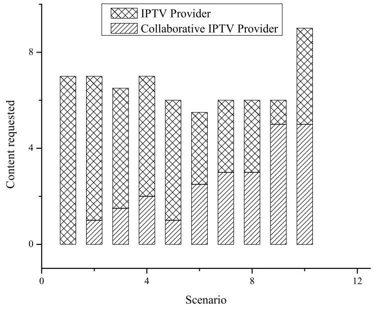

Fig. 7. SLA Adaptation service provision

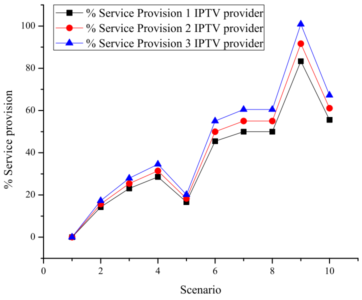

Fig. 8. Collaborative IPTV Provider percentage of service provision

whether to accept or reject service provision delegation. SSO efficiency is evaluated by means of traffic overhead i.e. the number of exchanged messages between IPTV provider and collaborative IPTV provider compare to the one caused by the combination of rejection and successfully getting the same content from alternative IPTV provider assuming mobile subscriber is a valid user for both security environments. In both scenarios we discriminate exchanged messages between entities. Results are summarized in Table 2.

Figure 8 shows the collaborative IPTV provider delivery percentage using SSO access control mechanism. It also represents the rejection percentage when SLA adaptation is not applied. The federation collaborative behavior allows dynamically balance the service provision and delivers efficiently the 100 percentage of timely-on demands.

5 Conclusions

In this work IPTV provider B2B scenario has been analyzed in order to identify access control and policies' multiple-attribute authorization requirements that M-IPTV framework needs for implementing an effective resource management mechanism for them to be able to guarantee the quality levels their customers demand during service provisioning. We have proposed the integration of new functionality to improve the flexibility of the management of SLAs in service provision. The resulting protocol exhibits a better performance in particular with higher rate of requests, that is, when capacity becomes a scarce resource increasing the rate of accepted requests and preserving the continuity of M-IPTV service provision.

Acknowledgments. This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency) (NIPA-2010-(C1090-1011-0001)) and by the IT R and D program of KCC/MKE/KEIT [Development of Open-IPTV Platform Technologies for IPTV Convergence Service and Content Sharing].

References

1. Burbridge, C.: Iptv the dependencies for success. Computer Law & Security Report 22(5), 409–412 (2006), `http://www.sciencedirect.com/science/article/B6VB3-4KTPS50-9/2/5f27baff7671b6ac5b02108eb23c7e57`
2. Chieng, D., Marshall, A., Parr, G.: Sla brokering and bandwidth reservation negotiation schemes for qos-aware internet. IEEE Transactions on Network and Service Management 2(1), 39–49 (2005)
3. García, D.F., García, J., Entrialgo, J., García, M., Valledor, P., García, R., Campos, A.M.: A qos control mechanism to provide service differentiation and overload protection to internet scalable servers. IEEE Trans. Serv. Comput. 2(1), 3–16 (2009)
4. Group, E.P.: Ebu project group b/ca: Functional model of a conditional access system. ebu technical review winter. Tech. rep., EBU Project Group (1995), `http://www.ebu.ch/en/technical/trev/trev_266-ca.pdf`
5. Group, E.P.: Ebu project group b/ca: Functional model of a conditional access system. ebu technical review winter. Tech. rep., EBU Project Group (1995), `http://www.ebu.ch/en/technical/trev/trev_266-ca.pdf`
6. Group, E.P.: Ebu project group b/ca: Functional model of a conditional access system. ebu technical review winter. Tech. rep., EBU Project Group (1995), `http://www.ebu.ch/en/technical/trev/trev_266-ca.pdf`
7. Hua, Z., Chunxiao, C., Li, Z., Shiqiang, Y., Lizhu, Z.: Content protection for iptv-current state of the art and challenges. vol. 2, pp. 1680–1685 (October 2006)
8. Jeong, J., Shin, D.: An xml-based security architecture for integrating single sign-on and rule-based access control in mobile and ubiquitous web environments. In: Meersman, R., Tari, Z., Herrero, P. (eds.) OTM 2006 Workshops. LNCS, vol. 4278, pp. 1357–1366. Springer, Heidelberg (2006), `http://dx.doi.org/10.1007/11915072_39`
9. Jeong, J., Shin, D., Shin, D., Oh, H.M.: A study on the xml-based single sign-on system supporting mobile and ubiquitous service environments. In: Yang, L.T., Guo, M., Gao, G.R., Jha, N.K. (eds.) EUC 2004. LNCS, vol. 3207, pp. 903–913. Springer, Heidelberg (2004), `http://dx.doi.org/10.1007/978-3-540-30121-9_86`

10. Lamanna, D.D., Skene, J., Emmerich, W.: Slang a language for defining service level agreements, pp. 100–106 (2003)
11. Lian, S.: Secure service convergence based on scalable media coding. Telecommunication Systems 45, 21–35 (2010), http://dx.doi.org/10.1007/s11235-009-9233-2
12. Lodi, G., Panzieri, F., Rossi, D., Turrini, E.: Sla-driven clustering of qos-aware application servers. IEEE Transactions on Software Engineering 33(3), 186–197 (2007)
13. Nishimoto, Y., Mita, N., Imaizumi, H.: Integrated digital rights management for mobile iptv using broadcasting and communications. IEEE Transactions on Broadcasting 55(2), 419–424 (2009)
14. OASIS: Organization for the advancement of structured information standards (oasis), http://www.oasis-open.org
15. OASIS: Saml v2.0 executive overview. Tech. rep., Organization for the Advancement of Structured Information StandardS (OASIS) (2005), http://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf
16. OASIS: Security assertion markup language (saml) v2.0 technical overview. Tech. rep., Organization for the Advancement of Structured Information Standards (OASIS) (2008), http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0-cd-02.html
17. Park, J.: Subscriber authentication technology of aaa mechanism for?mobile iptv service offer. Telecommunication Systems 45, 37–45 (2010), http://dx.doi.org/10.1007/s11235-009-9232-3
18. Park, S., Jeong, S.H., Hwang, C.: Mobile iptv expanding the value of iptv. In: International Conference on Networking, pp. 296–301 (2008)
19. Shin, D.H.: Potential user factors driving adoption of iptv. what are customers expecting from iptv? Technological Forecasting and Social Change 74(8), 1446–1464 (2007), http://www.sciencedirect.com/science/article/B6V71-4K7WJ16-1/2/8ef3650782581658cfebd54eb7c57207
20. Tiwari, P., Joshi, S.: Single sign-on with one time password, pp. 1 –4 (November 2009)