Management of Services in Ubiquitous Environments: using ontologies for dealing with quality-of-service

Renata Maria Porto Vanni, Edson dos Santos Moreira
Instituto de Ciências Matemáticas e de Computação
Universidade de São Paulo - Brasil
rporto,edson{@icmc.usp.br}

Abstract - Mobile and ubiquitous access to communication services have increased the need for more interaction between the providers. This interaction goes beyond the seamless access to the net; it must deal also with the controlling of the requirements of the content been transmitted. The core of the service providers interaction is a shared uniform structure which defines how managerial information is structured. One possibility, advocated in this work, is the use of ontologies. The research aims to develop an IT Management Ontology to provide a meaningful common vocabulary for the managerial information to be shared among service providers. Aspects of context awareness, quality-of-service, security, confidentiality, privacy and intellectual property right will form the kernel of the domain knowledge treated by the ontologies. It will be considered the sharing of the information as well as the privacy of sensible information of the business model for each provider. The work also concerns about creating the required process to enable the collaboration between the involved entities in the development, implementation, deployment and maintenance of the ubiquitous environment.

Index Terms— Ubiquitous Systems, Network Management, Quality-of-service, Ontologies, Information Systems, Security Information.

1. INTRODUCTION

The convergence and digitalization of the areas of radio, television, telephony and Internet have inspired the development of new wireless network technologies and the demand of new ubiquitous services for mobile devices. Many people are waiting for a portable device that offers a lot of functionalities like telephone, CD player, DVD player, e-mail, Web interface, gaming machine, word processor, and more, all with worldwide wireless connectivity to the Internet at high bandwidth[1].

Currently, the mobile devices receive intermittent network access, and alternate between connected and disconnected states. However, the increasing device networking capabilities and the ubiquity of wireless network coverage will make possible that always-on IP-based ubiquitous services become a reality.

The management of services in ubiquitous environments is more complex than the management of services in traditional environments. The complexity increase because of some situations that can occur when a mobile device changes its attached access point (handover) during the service delivery (Figure 1). These situations arise differently depending on the several views[2]:

- Technology view: handovers can occur between two access points that belong to the same technology (homogeneous handover) or different technologies (heterogeneous handover).
- Overlay view: handovers can occur between two access points belonging to the same network overlay (horizontal handover) or these access points belonging to different ones (vertical handover). Furthermore, if the old access point belongs to a technology with smaller coverage than the new access point we will have an upward handover - the opposite case is a downward handover.
- Domain view: an intra-domain handover occurs when the mobile device roam within the same network domain, but it can also cross more than one domain, executing an inter-domain handover.
- System view: when the mobile device roam between two independent systems - controlled by different network operators - this is an inter-system handover, and when the current and future access point are part of the same system it is a intra-system handover.

![Figure 1 – Handover taxonomy and views [1]](image)

The management system must deal with the different handovers and other aspects like:
The access points can be managed from different network management protocols (SNMP, CMIP), models (ITIL, CobiT, CMMI) and tools (HP ITSM, IBM ITSM, RMTG).

Business models of each provider with crucial information that must be protected during the exchanging of data for the handovers;

Specific policies for access, billing, privacy, security, quality-of-service and intellectual property right of each provider to be respected - if possible - and/or normalized by the mapping of properties.

The users of ubiquitous services will have seamless mobility but it is also desired to keep the quality-of-service (QoS) after the access point change and the fulfillment of the end-to-end Service Level Agreement (SLA) - Figure 2.

Many efforts are being made towards the integration of wireless network technologies, and of Information Technology and Communication Management models. For a complete solution some characteristics like QoS management must be treated[2].

The efforts - in Mobile Telephone System to the development of third-Generation mobile phones (3G) - are concerned about the future of mobile telephony (the devices and their connections), anticipating some factors[1]. First, many industry experts expect data traffic to dominate voice on mobile devices soon. Second, the convergence and digitalization of the areas of radio, television, telephony and Internet will demand service integration and ubiquity. The basic services supposed to provide to 3G mobile phone users are high-quality voice transmission, messaging, multimedia services and Internet access. Additional services might be video conferencing, telepresence, group game playing, and m-commerce. Furthermore, all these services are supposed to be ubiquitous, instantly, available worldwide, and with quality-of-service guarantees[1].

In order to reach IT management integration, some IT Service Management models like ITIL (Information Technology Infrastructure Library)[4,5], and IT Governance models like CobiT (Control Objectives for Information and related Technology)[6] have mappings between their management processes[3]. These mappings avoid the utilization of more than one model at IT Management and that they complement each other. But the syntactic translation in the mappings from the source model to the destination will not give the complete comprehension of the involved concepts. A semantic translation is necessary to give a common understanding of the domains’ concepts.[7]

The scenario described in Figure 1 and Figure 2 brought us some questions:

- How to control access on the boundaries?
- How (and where from) to gather the information needed for management?
- How to keep and map the QoS for the agreed SLA to the parameters of the new provider?
- How to deal with the different security, privacy, billing and intellectual property right policies of each provider?
- Who will request for the payment? Who is the owner of the bill?
- Whose help desk will the user complain to, in case of failure?

This work proposes to give the answers for some of these questions. The idea is to develop ontologies for the translations of the IT management models to support the continuous and integrated QoS and end-to-end SLA management, and to normalize information about the private policies of all service delivery chain. Some important reasons to develop an ontology are the following:

- The sharing of common understandings of a domain;
- The sharing of information structures;
- The reuse and extension of domain knowledge;
- The analysis of domain knowledge;
- The separation of domain knowledge and operational knowledge.

II. UBQUITOUS COMPUTING

The pervasiveness and the mobile nature of ubiquitous computing devices (Figure 3) require automatic, and ad hoc configuration from the network infrastructure. Other reason for support automatic configurations is that ubiquitous computing technology is aimed at ordinary consumers, who are not willing or not able to configure their devices manually[8].

L. Stojanovic et al. [10] proposed a set of ontologies in autonomic computing systems to deliver IT environments with improved self-management capabilities, such as self-healing, self-protection, self-optimization, and self-configuration. However, these ontologies not model other aspects of IT Management, such as the management of privacy, intellectual property right, quality-of-service, service level agreement, etc. Those information must be exchanged between service providers as the user migrates from a network to another.
The proposed semantic service management model in this work will require some properties that we believe it will be reach with the use of ontologies:

- to be flexible enough to handle seamless inter-provider handover information in terms of access control of policies of QoS, SLA, security, privacy, intellectual property right and billing;
- to be restrictive enough to hide crucial information which will keep the nuances of the business model of each provider in the service delivery chain;
- to be open enough so that providers can share some amount of information which will make the services to run as expected by the users when crossing providers borders;
- to be extensible enough to allow for the addition of the terminology from different sources;
- to be rich enough to provide proper information for CRM and alignment of the quality of the infrastructure and the businesses running over it.

III. WHY ONTOLOGY

The term “ontology” has been in use for many years, and it has several definitions; we quote 2 in here: (a) a branch of metaphysics concerned with the nature and relations of beings and (b) particular theory about the nature of being or the kinds of existences. These definitions provide an abstract philosophical notion of ontology[11]. Artificial Intelligence and web researchers have adopted this term for their own purposes. For them an ontology describes a formal, shared understanding of a particular domain that an use both by humans and systems to aid in information exchange and integration[10].

The use of ontologies has several advantages:

Interoperability. Ontologies provide a shared understanding of a domain, in our case the IT Management domain. In this way the concerns about the structural and semantic heterogeneity of different IT infrastructure can be solved. Structural heterogeneity happens when different IT Management store and manipulate their data in different schemas. Semantic heterogeneity involves intended meaning and management of information and its service relationships.

Ontologies provide an effective means for explicating implicit design decisions and underlying assumptions at IT management decision time. This makes it easier to reason about the intended meaning of the information exchanged between two or more providers. Therefore, interoperability is a key benefit of the application of ontologies.

Machine processability. Ontologies provide a formalization of shared understanding which allows machine processability and it forms the basis for the Semantic Web, which is itself based on using ontologies to improve the quality of content with formal semantics[12]. This will enable the implementation of IT management agents to reason about the services and carry out more intelligent tasks on behalf of the IT infrastructure.

New level of services. The explicit representation of the semantics of data through ontologies will enable the providers to reach an agreement with a qualitative new level of services, such as verification, justification, and gap analyses. The ontology axioms and rules provide the verification service, e.g. an agent can use axioms and rules to discovery the equivalent resource in other provider to give the necessary functionalities for the service interoperability. Justification refers to the generation of descriptions of the inference process to humans, i.e. how a result was inferred. Gap analyses is related to the incapacity for the discovery of IT infrastructure resources for the service interoperability, it is necessary for the continuous improvement and ontology extensibility and adaptability.

IV. ONTOLOGY DESIGN

The IT Management Ontology is a set of ontologies related to management of services in ubiquitous environments domain and it is based on the dimensions for the context of QoS and SLA.

The OWL (Web Ontology Language) will be used for the development of IT Management Ontology. OWL is an ontology language that evolved from languages like XML and RDF and it was designed for the Semantic Web. This language permits[13]:

- The description of a certain domain via the definition of classes and properties;
- The definition of the relationships existing among these classes and properties;
- The reasoning of the defined classes, properties and relationships, which prove the defined logic of the described domain, and verify its consistency.

OWL will permit additional semantic capabilities. For example, with RDF we can declare classes like User class, Service class and Client class, state that videoconference and e-mail are both instances of the class Service, and declare Nationality as a property relating the classes User (its domain) and Country (its range). Otherwise, with OWL we can state that User and Client are disjoint classes, state that John and Mary are distinct individuals, and declare HasCitizen as the
inverse property of Nationality.

Some classes that will be developed for the proposed ontology are Network_technology class, Network_management class, Service_management class, QoS class, SLA class, User class, Client class, Mobile_device class, Service_provider class, Content_provider class, Service class, Access_point class, Domain class, Handover_type class, Billing_policy class, Security_policy class, Privacy_policy class, Copyright_policy class, Who class, When class, Where class, What class, How class.

The User class will model the profile of all entities that can access services through a service provider. According to the example in Figure 4, the User class will have all relationships with Service class and Client class.

![Figure 4 - Classes and properties](image)

The SLA class will describe the Service Level Agreement that the client had signed with his service provider. The access attribute will list all services that the user can access.

The proposed ontology must be able to deal with context awareness, therefore must have some classes based on the W4H (who, when, where, what, how) dimensions for the context of IT infrastructure. For example, if the user (who) of an e-mail service is in the airport (where) at 12:00 p.m. (when) using a handheld (how) and he want to access his messages (what), then the ontology must provide the relations with this context and the privacy policies of the access provider.

V. FINAL REMARKS

The proposed ontologies will structure the managerial information for the sharing, common understanding and protection of the involved concepts in ubiquitous environments. The ontologies will permit the abstraction of managerial and exchanged information among providers and applications that will delivery the services with ubiquity and to protect vital information for one’s business. The model for structuring the data is somehow similar to that defined by the group developing the Nexus system [14], although there are no use of ontologies in that project. We believe that ubiquitous computing will demand well structured models to help the management of the quality-of-service guarantees and end-to-end SLA, and the normalization of policies for the service delivery.

ACKNOWLEDGEMENT

We are grateful to CAPES, a Brazilian Education Minister Agency, for the supporting for this work.

REFERENCES