Cloud-based framework for QoS monitoring and provisioning in consumer devices

Saša Radovanović, Norbert Nemet, Mića Ćetković
RT-RK Institute for Computer Based Systems
Novi Sad, Serbia
{sasa.radovanovic, norbert.nemet, mica.cetkovic}@rt-rk.com

Milan Z. Bjelica, Nikola Teslić
Faculty of Technical Sciences, University of Novi Sad
Novi Sad, Serbia
{milan.bjelica, nikola.teslic}@rt-rk.com

***Abstract*— The purpose of this paper is to provide a framework for a scalable, adaptable and efficient Quality of Service (QoS) monitoring system for consumer devices. The system is set in the Cloud environment and based on TR-069 remote management protocol. The proposed solution allows the development of secure, cloud-based network provisioning and management applications. Cloud access interfaces provide all needed information for the development of web-based or mobile applications which allow visualization of acquired QoS parameters.**

Index Terms*— *QoS, Service Level Agreement, Management, Provisioning, Consumer Electronics

I. Introduction

Consumer devices provide a variety of services to their users. The Quality of Service (QoS) concept has become vital for service providers. Users are becoming increasingly sensitive about the perceived quality of service [1]. Service providers need a development environment in which they can fulfill SLA (Service Level Agreement) obligations towards an increasing number of users within a sophisticated network environment. QoS is an instrument for continuous and proactive control of each service aspect in order to bridge the gap between the required and delivered quality. Existing solutions mostly insist on monitoring the content sent by the provider and not the content received by the user since the information sent by the provider is subject to interference and network congestion and thus not necessary received unaffected.

The most effective QoS requires feedback from each user regardless of the network type or the parameters monitored [2]. Modern QoS provisioning must allow network supervision based on passive and active monitoring. This feature demands a protocol between the end-user and the monitoring system for a continuous insight into QoS to prevent manual troubleshooting of potential issues. Modern systems are high on demands for resources. Therefore, monitoring modules require large processing power with storage capabilities for conservation of data received. In this paper QoS monitoring and control framework is proposed to provide means for the providers to answer the always growing support demands in terms of QoS.

II. System Architecture and Development Framework

Key components of the framework are QoS Cloud Server and QoS User Provisioning (QoS UP) library. QoS Cloud Server is deployed as a platform (PAAS). The framework is designed to be independent of the specific network and the nature of exchanged parameters. Framework seeks to provide an efficient way for providers to personalize, scale and implement requirements based on the characteristics of end-devices. It allows them to specify service parameters they want to monitor through the proposed QoS UP library. Parameters are automatically returned by the end-device. Core technology of the QoS Cloud server is based on the application server with modular storage unit implemented using database and cache. Using object-related mapping library, the framework is made independent from the version of database used. Frequently accessed data are stored to cache using distributed data grid platform. Used technologies provide scalability and distributed data processing along with an abstraction of physical parameters through the concept of Data Processing modules. Architecture of the framework is shown in Fig. 1.

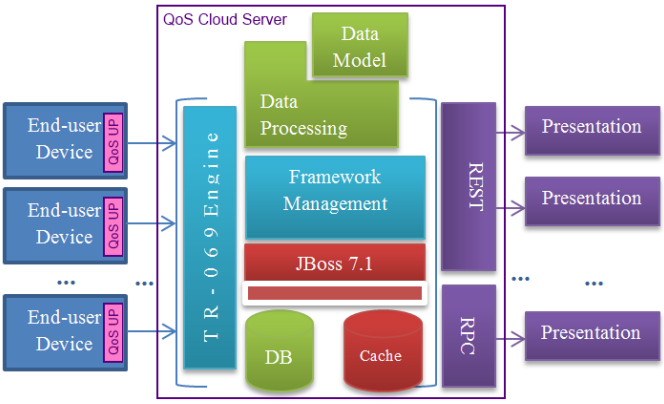

Figure 1. Top-level architecture.

QoS Cloud Server provides two different APIs for application development. The first API is dedicated to the consumer end-devices (CPEs – Customer Premises Equipment using TR-069 protocol). The second API is reserved for presenting information processed by the Cloud Server. TR-069 (also known as CPE WAN Management Protocol) is selected as a protocol for consumer end-devices since it provides means for

parameter exchange and monitoring regardless of network infrastructure. The API used by presentation modules is implemented using Remote Procedure Calls (RPC) and REST mechanisms. These allow for acquisition of data at any given refresh rate.

III. Security

The framework provides security mechanisms and reputation-based trust management to secure public domain data flow [3]. Both communication layers of the framework provide end-to-end security with HTTPS/SSL. End users and presentation clients use different message types with adapted security mechanisms. TR-069 top level messages use SOAP format, therefore it is advised that WSS (Web Services Security) should enforce the integrity of communication [3][4]. WSS mechanism ensures encryption of SOAP based messages thereby every data exchanged between framework and end users is preserved from illegal usage. This adds new level of security and proposes a solution to TR-069 vulnerability to third party intrusions. On the other end, access to user data is controlled by account access control, with policy defined by the provider. Federated Identity Management (FIdM) is implemented using PAM (Pluggable Authentication Module) mechanism which enables high level applications to recognize different controllers of the framework with different access privileges. Besides specifically securing both communication ends, framework is applying Cloud-specific security mechanisms through corrective and detective controls.

IV. Evaluation

System was evaluated in an environment of DVB-T2 set-top-boxes (STBs) as the end user devices. Tested network is in adapted star network topology. Android and Web based applications were used as presentation tools. The framework showed stability and robustness with a high number of user devices in field tests while retaining acceptable reaction to notifications. Customized Data Processing allows presentation clients to visualize advanced features such as signal quality heat map based on geographical information or signal quality history for a specific end user as shown in Fig. 3. One evaluation scenario insisted on determining the response time from Server to presentation clients which ask for the QoS signal quality parameter in function of the number of end devices as shown in Fig. 2. Another test scenario shows Server response time towards end-user devices in getting value of certain parameters and setting their value. The test case was performed 20 times in order to determine fluctuation of response time in network consisting of 2500 end devices. The results are shown in Fig. 4. Obtained results indicate acceptable response time which is not severely affected by the number of devices handled by the QoS server on both ends, what shows the feasibility of the proposed solution for the typical QoS monitoring scenarios.

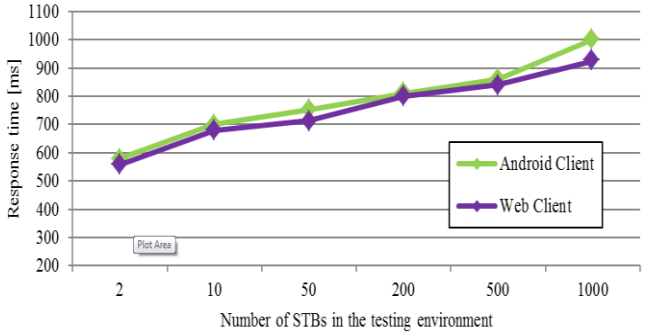

Figure 2. Response time towards presentation clients.

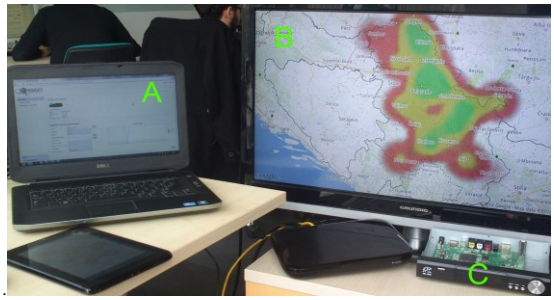

Figure 3. Testing environment (A –Web-based presentation client, B – Heat map on Android presentation client, C – STB with QoS UP library).

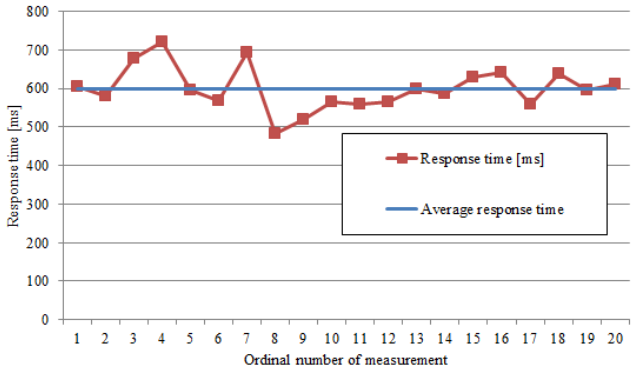

Figure 4. Response time towards end-users.

V. Related Work

QoS in networks is a main subject in many research works. However, most are not consumer device oriented. In the concept of distributed SLA [5], measurement based on client feedback is introduced. That model is accepted and modified to suite the nature of device types. The importance of flexibility is mentioned in [6] as feature for successful QoS management. We endorse and expand that paradigm. More works emerged with Cloud computing becoming an option for remote resources. Several monitoring systems propose solutions for large distributed systems. To the best of our knowledge, present solutions fail to provide the unique and scalable development environment for the facilitated creation and maintenance of custom QoS monitoring platforms. They have problems with dynamics of infrastructure but provide a base for research such as [7]. The framework managing self-configuring devices is presented in [1]. It is based on the TR-069 protocol providing an environment for high performance

networks, although it does not provide a solution for connecting presentation tools. The Internet of Things (IoT) is an upcoming concept, with requirements and end-user QoS architecture being proposed in [8]. It proposes solution for some main architecture issues and provides a base for integrating QoS in IoT objects. Framework proposed in this paper is complementary with that architecture. Modernized electrical grids are dependent on reliable QoS monitoring. Solution for QoS monitoring of SmartGrids is proposed in [9]. It presents a proposal for integrating QoS modules in SmartGrid entities. This framework provides an extension for monitoring those entities.

VI. Conclusion

QoS monitoring for consumer devices based on Cloud computing will be a primary choice for the time to come. Our solution provides a cloud-based development platform for QoS for different types of consumer devices. It also provides a solution for upcoming energy distribution models and IoT networks complying with specific QoS requirements [10][11]. Conducted evaluation suggests that the approach is feasible for large numbers of devices monitored. Special attention is given to covering security issues and supporting dynamics in high performance networks regardless of device type. Future work will insist on increasing security measures all over the framework and expanding the set of monitored QoS parameters.

Acknowledgment

This work was partially supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia under the project 44009, year 2011.

References

[1] H. Rachidi, „A framework for self-configuring devices using TR-069“, Int. Conf. on MCS, Morocco, 2011.

[2] R. Jurca, W. Binder, B. Faltings, „Reliable QoS Monitoring Based on Client Feedback“, pp. 1003-1010, Int. Conf. on WWW, USA, 2007.

[3] K. Hwang, S. Kulkureni, Yue Hu, „Cloud Security with Virtualized Defense and Reputation-based Trust Management“, Int. Conf. on DASC, Chengdu, China, 2009.

[4] S. Ramgovind, M.M. Eloff, E. Smith, „The Management of Security in Cloud Computing“, ISSA, South Africa, 2010.

[5] A. Sahai, V. Machiraju, M. Sayal, A. Van Moorsel, F. Casati, „Automated SLA monitoring for Web Services“, 13th IFIP/IEEE Int. Workshop on DSOM, pp. 3-11, Canada, 2002.

[6] R.E. Schantz et al., „Flexible and Adaptive QoS Control for Distributed Real-Time and Embedded Systems“, Int. MW Conf., Brazil, 2003.

[7] R. Grati, K. Boukadi, H. Ben-Abdallah, „A QoS Monitoring Framework for Composite Web Services in the Cloud“, Int. Conf. on AECAS, pp. 65-69, Spain, 2012.

[8] Ren Duan, Xiaojiang Chen, Tianzhang Xing, „A QoS Architecture for IOT“, International Conference on and 4th International Conference on Cyber, Physical and Social Computing, China, 2011.

[9] Wei Sun et al., „Quality of Service Networking for Smart Grid Distribution Monitoring“, IEEE International Conference on Smart Grid Communications, USA, 2010.

[10] Zhou Ming, Ma Yan, „A modeling and computational method for QoS in IOT“, China, 2012.

[11] Yong-Hee Jeon, „QoS Requirements for the Smart Grid Communications System“, International Journal of Computer Science and Network Security, VOL.11 No.3, 2011.