APPLICATION OF WEB SERVICES FOR SOFTWARE DEFINED RECONFIGURABLE EQUIPMENTS

Bertrand Souville (DoCoMo Euro-Labs, Munich, Germany, souville@docomolab-euro.com)

ABSTRACT

The convergence of Internet and mobile networks is foreseen in future wireless communication systems. Software defined reconfigurable equipments have the capabilities to change their configuration by software upgrades. In this paper, it is assumed that software upgrades may affect multiple layers in the protocol stack and may involve several software providers. Web Services is considered as adequate technology for the software upgrade of reconfigurable equipments. The building blocks of Web Services are SOAP, WSDL and UDDI and these technologies are included in the proposed software upgrade architecture. Security matters related to the defined architecture are also considered. Finally, the implementation and future work are outlined.

1. INTRODUCTION

A large number of mobile computing devices can be connected to the Internet via cellular networks, wireless LANs and wireless MANs. In the future, the adoption of a common IP backbone that interconnects heterogeneous access networks is envisioned. Software defined reconfigurable devices will switch between different air interfaces and facilitate the access to the wireless Internet irrespective of the access technology or the point of connection used (See figure 1).

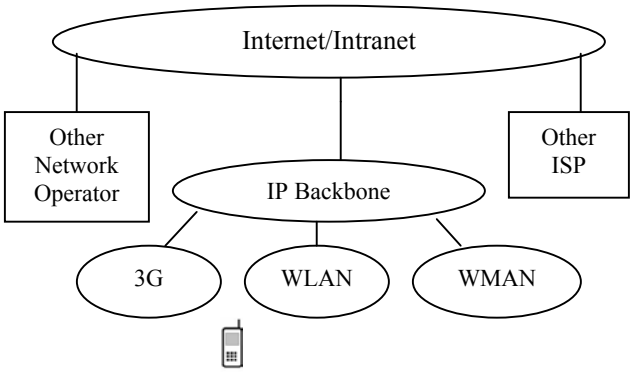

Figure 1. Convergence of Internet and mobile networks

The software upgrade of reconfigurable devices affects all layers in the protocol stack. Previous work assumes that the transfer of the software will be done over the air from central servers in mobile networks or by peer-to-peer based techniques [1]-[4]. The complexity associated with the software upgrade of reconfigurable equipments depends on several parameters:

- **Nature of the upgrade**. The download of software that controls RF parameters has more security requirements and regulatory implications than the download of higher layer software. Moreover, the upgrade may involve several software providers in the case of the reconfiguration of multiple layers in the protocol stack.
- **Number of reconfigurable equipments affected by the upgrade**. The installation of new protocols in reconfigurable devices may require the upgrade of network equipments. Synchronization of upgrades is a key issue.
- **Number of responsibility entities for the upgrade**. It is expected that the equipment manufacturer will take a central role for the integrity of the reconfigurable equipment.
- **Regulation rules for reconfigurable equipments** will have to be taken into account with regard to equipment approval [6].

In this paper, it is considered that the mobile users will retrieve the software upgrades from the Internet or from Intranets. This approach is quite new and has three major advantages:

- Similar to the upgrade of personal computers, mobile users will use their browser and select appropriate software upgrades according to their requirements.
- Ubiquitous access services to Internet are currently proposed in both licensed and unlicensed bands of spectrum by network operators and wireless Internet service providers (ISP).
- The time for the transfer of large amount of software can be reduced by employing a combination of high speed wired transmission technology and short-range wireless transmission technology.

Web Services is proposed as adequate technology for the software upgrade of reconfigurable equipments. The remainder of the paper is organized as follows: Section 2 provides our architecture proposal. In section 3, security considerations will be further developed. In section 4, the implementation will be shortly presented.

2. WEB SERVICES FOR THE SOFTWARE UPGRADE OF SDR EQUIPMENTS

2.1 Definition of Web Services

Web Services allows business interactions on the Internet and Intranets where business services can be described, discovered, published and utilized dynamically in a distributed environment. In the context of the upgrade of SDR equipments, the interaction model between the business entities is shown in figure 2.

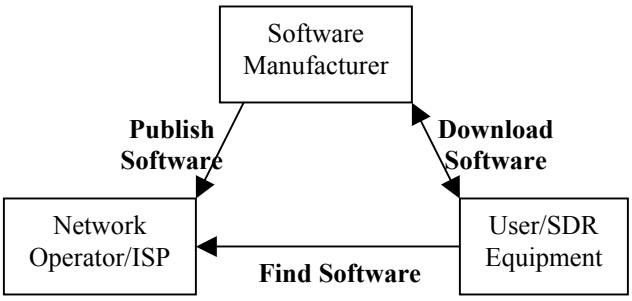

Figure 2. Interaction model for the software upgrade

The following business entities are defined:

1. The software manufacturer is the service provider and publishes the software in a registry. The service offered includes the list of previously approved software by relevant authority and the list of hardware platforms supported.
2. The network operator or Internet service provider acts as a broker and finds relevant software modules on behalf of the SDR equipment based on the current configuration and capabilities of the SDR equipment.
3. The SDR equipment or the user is the service requestor and interacts with the service provider based on the information provided by the broker.

The following standardized Internet technologies are the building blocks to describe, find and use Web Services [7]:

- The Simple Object Access Protocol (SOAP) is a protocol that defines the way of passing XML data. Basically, the interactions between the service requestor and the broker consist of an XML request and an XML response.
- The Web Services Description Language (WSDL) is an XML language that provides a way to describe what a Web services can do, where it resides, and how to invoke it.
- The Universal Description Discovery and Integration (UDDI) provides a mechanism for brokers to dynamically find Web Services. Currently, a UDDI registry is used for the interactions between the broker and the service provider.

2.2 Software Upgrade Architecture

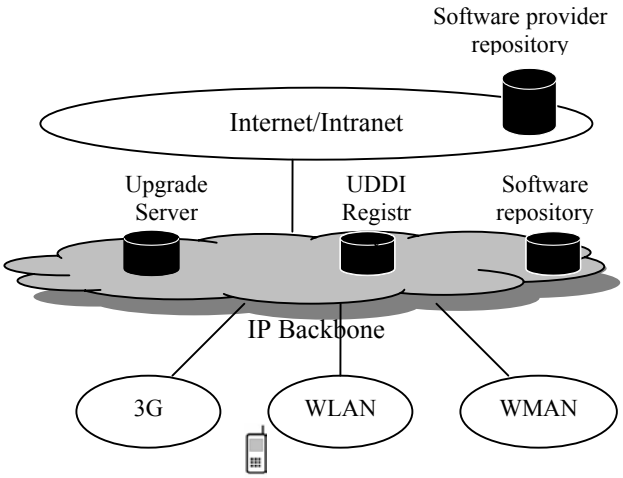

Figure 3. Software upgrade architecture

Figure 3 presents the proposed software upgrade architecture. Software providers (including network operators) store their WSDL document in the UDDI Registry located in the IP backbone. The WSDL document consists of the list of approved software modules and hardware platforms supported plus the messages that must be exchanged to successfully interact with the software providers. The upgrade server is responsible for the following tasks:

- Based on the software upgrade request coming from the SDR equipment, the upgrade server finds the appropriate software modules.
- The upgrade server checks the validity of software modules.
- If the software modules originate from multiple software manufacturers, the upgrade server collects all software modules and transfers them to the SDR equipment. Otherwise, it sends back software provider information (e.g. binding information).

3. SECURITY CONSIDERATIONS

3.1 Security Objectives

Security for the software upgrade of SDR equipments is covered in the industry and by regulatory authorities [4]-[6]. It is generally recognized that the security aspects of the software download depend on the layer of the protocol stack considered. A number of standardization bodies such as IETF, the Open Mobile Alliance and 3GPP improve the security for mobile Internet but a number of research challenges remain due to the heterogeneity nature of the access network technologies and various security

mechanisms employed at different layers of the protocol stack. In this paper, the following security objectives will be considered:

- Secure (confidentiality and integrity protection) exchange of SOAP messages. SOAP messages should not be altered nor be readable during the transfer. For instance, the SOAP request originating from the SDR equipment may contain critical information (e.g. configuration information of the SDR equipment) and should be kept confidential.
- Non-repudiation. The software upgrade is a business transaction among software providers, network operators/ISP and SDR equipments. Non-repudiation needs to be guaranteed.
- Access control policies to the Registry. It must be ensured that software providers have granted rights to access the Registry.

3.2 Discussion

Security extensions for SOAP have been created and provide transport-agnostic security measures. The OASIS Web Services Technical Committee [8] currently defines SOAP Encryption (SOAP-ENC) and SOAP Signature (SOAP-SIG) as part of the SOAP Message Security Specification .

SOAP Encryption provides two advantages in comparison with transport-level confidentiality solution such as SSL: Firstly, SOAP Encryption can encrypt only parts of the message using a symmetric key. Secondly, it can integrate different security domains with various transport-level security solutions (e.g. SSL in Internet and WTLS in mobile networks).

SOAP Signature appends digital signatures to the SOAP message for integrity purposes and in order to authenticate the creator of the SOAP message. SOAP Signature is not sufficient for non-repudiation. Indeed, digital signatures do not guarantee that the creator of the SOAP message coincides with the sender of the message: A malicious entity may intercept the message and claims that it is the creator of the SOAP message when re-sending it to other entities. Therefore, underlying security mechanisms such as mutual client/server authentication combined with SOAP signatures are required for non-repudiation purposes.

As defined in the UDDI specification [8], access control to the registry may be performed by the definition of policy rules:

- Registration policies have to be implemented by the registry to specify how software providers may publish their software modules.
- Authorization policies have to be implemented by the registry to specify which software providers may have access to the registry.

These defined security extensions are required to ensure the underlying trust between the software providers, the network operators and the SDR equipments. Further study is also planned to address other specific requirements for secure software download such as the definition of countermeasures against illegal copies of software upgrades [9].

4. IMPLEMENTATION

This implementation of the software upgrade platform was motivated by previous work on reconfigurable mobile nodes in ad hoc networks [10]. The Java platform was selected for portability reasons. Moreover, the Java Web Services Developer Pack includes APIs and technologies to easily build Web Services. As shown in figure 4, the implementation architecture includes the building blocks of the Web Services. HTTP was chosen as the underlying transport protocol for the exchange of SOAP messages.

In ad-hoc networks, the reconfiguration of mobile nodes may be triggered by evolving mobility characteristics requiring the change of routing protocols [10].

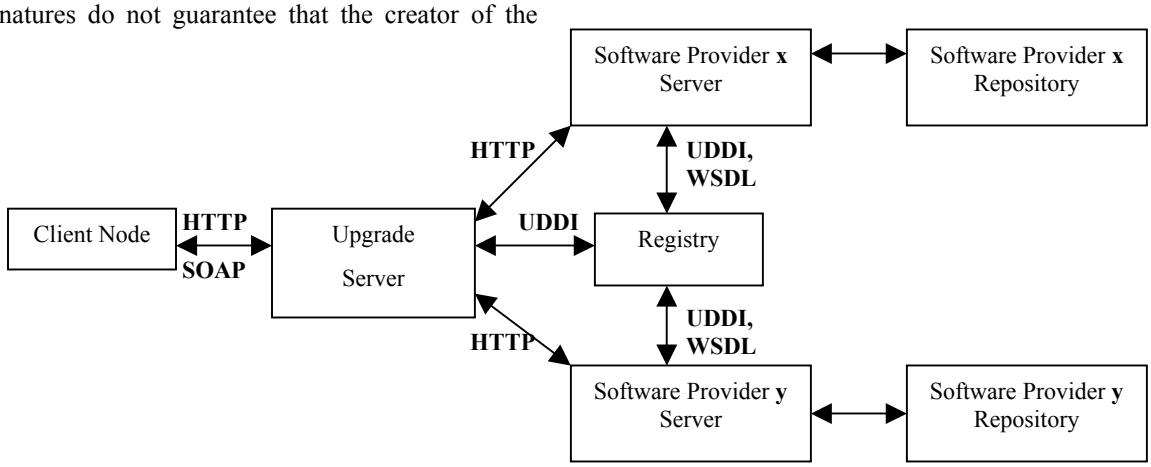

Figure 4. Implementation architecture

It is assumed here that one node has access to Internet and has deployed the upgrade server and the registry. All other nodes act as client nodes.

Figure 5 presents the sequence diagram illustrating the interactions between the entities defined in the implementation architecture.

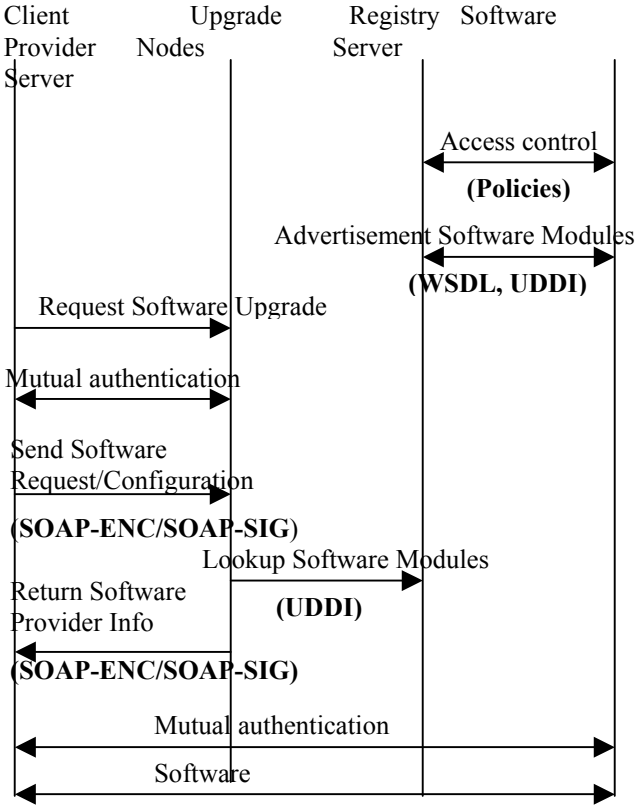

Figure 5. Sequence diagram

5. SUMMARY

We have considered the applicability of Web Services for the software upgrade of reconfigurable equipments. The complexity of the upgrade and related security matters are greatly increased when the software modules are located in the Internet and originate from different software providers. Web Services security extensions address some of the security objectives in terms of integrity and confidentiality of exchanged SOAP messages.

6. REFERENCES

[1] H. Shiba, T. Shono, K. Uehara, S. Kubota, "Design and Evaluation of Software Radio Prototype with Other-the-Air Download Function", Vehicular Technology Conference, IEEE, Volume 4, pp. 2466-2469, 2001

[2] K. Moessner, R. Tafazolli, "Terminal reconfigurability – The software download aspect", 3G Mobile Communication Technologies, pp. 326-330, 2000

[3] M. Dillinger, R. Becher, "Decentralized software distribution for SDR terminals", IEEE Wireless Communications, Volume 9, Issue 2, April 2002

[4] T. Farnham et al., "IST-TRUST: A perspective on the Reconfiguration of Future Mobile Terminals using Software Download", Personal Indoor and Mobile Radio Communications, vol. 2 , pp. 1054-1059, 2000

[5] L.B. Michael, M. J. Mihaljevic, S. Haruyama, R. Kohno, "A framework for secure download for software-defined radio", IEEE Communications Magazine, Volume 40, Issue 7, pp. 88-96, July 2002

[6] Federal Communications Commission, "First report and order in the matter of Authorization and Use of Software Defined Radios", ET Docket No. 00-47, September 2001

[7] F. Curbera et al., "Unraveling the Web Services Web. An introduction to SOAP, WSDL, UDDI", IEEE Internet Computing, March-April 2002.

[8] www.oasis-open.org OASIS Web Site

[9] M. Sugita, K. Uehara, S. Kubota, "Flexible Security Systems and a New Structure for Electronic Commerce on Software Radio", Vehicular Technology Conference, Volume 6, pp. 3033-3040, Sept. 2000

[10] C. Prehofer, B. Souville, "Synchronized reconfiguration of a group of mobile nodes in ad hoc networks", ICT 2003, pp. 400-405, Feb. 2003