Computer Communications 68 (2015) 33–46

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Contextualising heterogeneous information in unified communications with security restrictions

Ana Nieto*, Javier Lopez

Computer Science Department, University of Malaga, Ada Byron building, 29071 Malaga, Spain

ARTICLE INFO

Article history:
Available online 16 July 2015

Keywords:
Security
QoS
Tradeoff
Context

ABSTRACT

The lack of abstraction in a growing semantic, virtual and abstract world poses new challenges for assessing security and QoS tradeoffs. For example, in Future Internet scenarios, where Unified Communications (UC) will take place, being able to predict the final devices that will form the network is not always possible. Without this information the analysis of the security and QoS tradeoff can only be based on partial information to be completed when more information about the environment is available. In this paper, we extend the description of context-based parametric relationship model, providing a tool for assessing the security and QoS tradeoff (SQT) based on interchangeable contexts. Our approach is able to use the heterogeneous information produced by scenarios where UC is present.

1. Introduction

Future Networks are intended to be convergent networks, where multi-purpose devices can coexist and cooperate to achieve common goals, or even work in an opportunistic symbiosis. Therefore, *Unified Communications* (UC) play an important role by opening the door of the collaboration between heterogeneous devices in different environments [1]. This entails several challenges, for example, what happens to the valuable information generated by the collaboration, how it can be used and also protected and, moreover, how to handle the different environments to be analysed to identify the dependencies between the parameters that may be critical (e.g., for identifying cascade effects). Furthermore, in *Future Internet* (FI) scenarios, where multiple devices coexist and networks are always changing, performing tests or simulations before the deployment of the solutions is very complex, because the number of factors to be considered and measured increase exponentially. We are especially concerned about security and Quality of Service (QoS) mechanisms, because both are fundamental in providing a total network convergence [2].

Some of the challenges regarding the security and QoS are motivated by the users' growing demands, the unification of heterogeneous and dynamic environments, and the problems in predicting the behaviour of the final ecosystem. Users' applications and services necessarily require the existence of both, QoS and security mechanisms [3,4], in order to guarantee, atleast to some degree, that the network will be able to satisfy the user's demand for performance (e.g., delay, response time) and security (e.g., privacy, integrity, confidentiality). Furthermore, the capability of providing QoS or security mechanisms also depends on the resources of the environment (e.g., bandwidth, coverage provided by the antennas) and the resources of the devices (e.g., memory, security architecture). In general, not all the mechanisms can coexist in the same environment without affecting each other.

Moreover, the user's mobility between different domains complicates the traceability of malicious devices, and poses serious challenges to the resource provisioning, that are based on the predictability of being efficient. In this respect, in [5] the authors provide an interesting map and classification of where the data in cellular networks is located and generated. This information is not only personal, but also includes measurements about the performance of the mechanisms in the network which can be stored and analysed to improve the configuration of the systems and to predict when the peaks of demand of resources occur.

Therefore, as more systems converge, more information is available to understand the behaviour of the network and to be used to analyse the security and QoS tradeoff [6]. This analysis must to be done considering partial information, because the dynamic nature of these environments reveals the requirements, properties and characteristics to be considered, but not the final mechanisms that must be available for implementing the security and QoS requirements. For example, in ad-hoc communications, the solutions to be deployed depend a lot on the capabilities of the devices. If the devices do not support the communication protocol, then diverse security and QoS mechanisms cannot be applied [7]. Moreover, as the user is included

* Corresponding author. Tel.: +635363636.
E-mail addresses: nieto@lcc.uma.es (A. Nieto), jlm@lcc.uma.es (J. Lopez).

http://dx.doi.org/10.1016/j.comcom.2015.07.015
0140-3664/

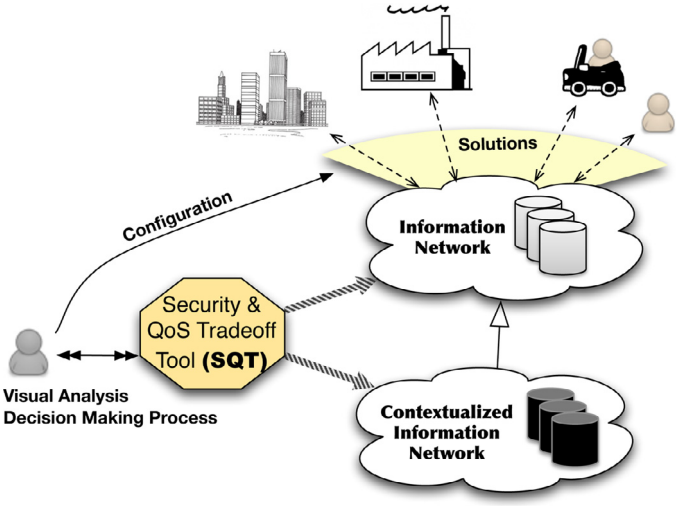

Fig. 1. Security and QoS Tradeoff Tool.

as part of the network, and is able to interact with the things or objects around him/her, new solutions should be deployed and configured considering a wide range of purposes in mind, based on a context, where subjective values have to be considered. The subjectivity of a component is essential, to identify the components or things that are fundamental to a user, or any other actuator in the network, at any given moment.

We define the *generic models for assessing the security and QoS tradeoff* as those models capable of analysing the security and QoS requirements and characteristics of a set of elements and components in a system. These models are capable of changing the composition of these elements and characteristics for others and still be useful. The idea behind these types of models is that a part of the model has to remain abstract prior to knowing or receiving the new components in the information system. So, these models are well suited to use in heterogeneous networks of dynamic composition, as is the case of UC in FI environments, where it is very difficult to predict with any great accuracy the devices that will comprise the network.

In this paper we define a tool for assessing the *Security and QoS tradeoff* (SQT) in heterogeneous networks, taking as the basis, a set of well defined security and QoS parameters and their relationships, expressed as part of a *Context-based Parametric Relationship Model* (CPRM). The mathematical formulation for the CPRM model was initially defined in [8], as well as a basic description of the behaviour of the model. Here we extend the description of the behaviour of the model and focus on the requirements to develop the tool according to the model. This extension is necessary to detail the modelling of SQT, which was built based on what we consider to be the key requirements for analysing the Security and QoS tradeoff in future networks. SQT is considered as a handler for CPRM-based systems, and, in this paper, the steps for developing similar tools to SQT are provided[1]. Fig. 1 shows the idea behind SQT. It is a knowledge-based tool that uses the information on the environment to provide information about the security and QoS parameters and relationships.

The paper is structured as follows. Section 2 introduces the related work. Section 3 defines the CPRM model, defining the basic behaviour that should be implemented and the requirements for the integration of different contexts. Section 4 explains the steps that have to be taken to build SQT, based on the requirements imposed by the model. Section 5 provides the definition of the use case to be implemented in the analysis in Section 6. Our conclusions and future lines of research are given in Section 7.

[1] In our case, we provide a prototype built in MATLAB that cannot be adapted to all the environments, but that we consider is very useful to understand the basic usability of SQT.

2. Related work

Analysing the current contributions it is possible to identify a set of trends in the analysis of security and QoS tradeoffs. Most of these contributions focus on service composition/selection, as in [9], where model checking techniques are used to verify the composition of security services, or in [10], where a tool for evaluating the composition of security services based on *Multi-Objective Optimisation* (MOS) is provided. In [11] trust and QoS tradeoffs are analysed for web services composition. In this case, the selection of services concentrates on general services (not necessarily security services), and trust is a property of the services that must be considered during the agregation of services. In [12] the composition of security services is proposed for *Software Defined Networks* (SDN), where high-level approaches are feasible. Security is seen in some approaches like [13], as a requirement to protect the network against *Denial of Service* attacks for ensuring the QoS. In [14] an approach to provide security in SDN considering QoS guarantees is presented. Moreover, the security and QoS tradeoffs are also a problem in resourced-constrained environments that are connected to the Internet [11,15]. In these environments defining the parameters, operations and the rest of the components and properties within a context, is key in identifying their relevance in the final composition of elements in the environment [16]. Alternatively, in [17] a model based on three static contexts (computing, physical and user) is defined based on a utility function in order to consider the user's preferences to capture fine-grane tradeoffs between security and QoS.

We conclude that most of the current approaches (i) focus on specific objectives (security and QoS tradeoffs using specific parameters or at specific layers, typically at the service layer), (ii) define generic models but do not consider partial-knowledge of the environment (it is not always possible to predict the final mechanisms that will implement the properties), or (iii) do not consider the subjective perception of the user (what the user wants is not always best, but it is what they want).

We advocate assessing security and QoS tradeoff based on the analysis of parametric relationships, separating the parameters based on their type, different layers of abstraction and subjective values needed in the dynamic FI that affect the UC. These parametric relationships have to correctly define the dependencies between the security and QoS parameters. Our approach considers the composition of *things*, in that sense. We are not only interested in the services, but also in the low-layer characteristics or technologies that can be used to increase coexistence and cooperation in the network between the security and the QoS mechanisms.

3. Behaviour based on the context-based parametric relationship model

In order to combine the analysis of diverse mechanisms to provide security and QoS under a common framework, in [8] a *Context-based Parametric Relationship Model* (CPRM) is defined. The model defines the structure that a dependency-based system should have in order to provide useful information for analysis from a tradeoff perspective. It also defines the steps required to integrate new dependencies based on new conditions, to provide a new context. So, finally, the superposition of contexts, defines the new behaviour of the system, and this behaviour can be analysed based on a set of well-defined dependencies. In this section we extend the definition of CPRM to identify the basic requirements to build SQT.