A. Nieto, and J. Lopez, "A Model for the Analysis of QoS and Security Tradeoff in Mobile Platforms", *Mobile Networks and Applications (MONET) Journal*, vol. 19, pp. 64-78, 2014.
http://doi.org/10.1007/s11036-013-0462-y
NICS Lab. Publications: https://www.nics.uma.es/publications

A Model for the Analysis of QoS and Security Tradeoff in Mobile Platforms

Ana Nieto · Javier Lopez

Abstract Today, mobile platforms are multimedia devices that provide different types of traffic with the consequent particular performance demands and, besides, security concerns (e.g. privacy). However, Security and QoS requirements quite often conflict to a large degree; the mobility and heterogeneous paradigm of the Future Internet makes coexistence even more difficult, posing new challenges to overcome. Probably, one of the main challenges is to identify the specific reasons why Security and QoS mechanisms are so related to each other. In this paper, we present a Parametric Relationship Model (PRM) to identify the Security and QoS dependencies, and to elaborate on the Security and QoS tradeoff. In particular, we perform an analysis that focus on the mobile platform environment and, consequently, also considers subjective parameters such user's experience, that is crucial for increasing the usability of new solutions in the Future Internet. The final aim of our contribution is to facilitate the development of secure and efficient services for mobile platforms.

Keywords Security · QoS · dependencies · relationships · parameters · tradeoff

1 Introduction

Today personal mobile devices are essential in the life of many people. In fact, they are designed taking into account several social factors and market studies in order to increase the user satisfaction and encourage their use. Thus, with the integration of new paradigms such as social networking, users are even more dependant on technology in order to be always-on.

However, as in the case of personal computers, when mobile devices connect to the Internet or any other public network, new features become available to the users, but also numerous threats against which they need to be protected. Thus, Security and *Quality of Service* (QoS) tradeoff consists of providing security mechanisms while also guaranteeing the quality in the communication and network performance. Unfortunately, unlike personal computers, mobile devices are resource-constrained and traditional QoS mechanisms cannot be directly used. The same is true for security mechanisms as they are difficult to apply without degrading the overall performance of the mobile phone.

As a consequence, in the current environment, both security and QoS researchers consider network performance as a precious resource, and several approaches in both areas, separately, have aimed to improve the network (e.g. delay) and local (e.g. battery) performance. Actually, even Security is considered to be QoS parameter (e.g. deliver secure traffic with a certain priority or privacy to increase user's satisfaction). However, there are few research works that have jointly studied Security and QoS tradeoff while addressing Security and QoS as two separate and independent concepts. Indeed, this is key to understand the main problems in the future development of solutions (mechanisms, applications, hardware) in mobile platforms.

Moreover, Security and QoS tradeoff in mobile platforms is present in different contexts (e.g. new developments, network attacks) and this complicates the analysis of interdependencies between related parameters and requirements. Such an analysis may provide useful data about the influence and dependence among parameters or sets of parameters, which is the first step

Computer Science Department, University of Malaga (Spain)
Tel.: +34-952-134186
Fax: +34-952-134184
E-mail: {nieto,jlm}@lcc.uma.es

in order to find countermeasures that avoid the unbalanced Security and QoS scenarios which degrade user's experience. However, this is a difficult issue, because the number of parameters increases even more when the user is involved. Moreover, the contextual differences among parameters increase too.

For example, a relevant topic discussed regarding the security in mobile platforms is the analysis of attacks and threats [1] [2] [3] that, while related with the QoS and performance, plays an important role in user's experience and more generally in *Quality of Experience* (QoE) [4] [5] [6]. In the first case, security parameters could be related with a particular algorithm or configuration for an algorithm (e.g. use encryption), or even a security requirement (e.g. authentication), but in the QoS context a requirement may aim to ensure the jitter under a threshold defined by the application or the service, or, to increase the perception of a set of users on the boundary of a particular service.

Hence, different parameters in different contexts may not be related, but in a real environment they have to coexist because they are part of the same general environment: mobile platforms.

Intuitively, the parameters cannot be set according to particular contexts because, sometimes, contexts overlap (e.g. Security in Handover scenarios). Instead, we consider that the parameters should be classified based on different layers which represent different roles or levels of abstraction within the mobile platform's infrastructure. In particular, and as shown later, we divide our analysis into five main layers, according to the location of the parameters in a given mobile scenario: High-Level Requirements, Local Properties, Communication, Measurements and Environment.

1.1 Motivation

The main objective behind the work presented here is to provide an analysis of Security and QoS tradeoff in mobile platforms based on the analysis of interdependencies. This paper is a sustainable extension of our previous paper [7], where the *Parametric Relationship Model* (PRM) was defined (though not implemented). In the actual version, the parameters set is increased, so a decomposition of the problem into layers is proposed in order to address the difficulty of working with large parameter sets, and the dependencies diagram is built for each layer based on the PRM. The PRM has been implemented using MATLAB, and the Security and QoS tradeoff has been analysed using it. In this way, from the dependencies diagram focused on mobile platforms, we extract relevant information for discussion.

The analysis also considers the effect that such dependencies have on the QoE measures, with the aim of considering both QoS and user's perception. Indeed, it has been clearly demonstrated that security mechanisms tend to consume network and local resources and can easily affect the normal performance of devices, which in turn can have a negative effect on user's satisfaction [5]. This is very dangerous in a personal device from the point of view of progress and business. Therefore, in this paper, we use the concept of QoE to take into account not only the QoS, but also user's experience.

1.2 Security and QoS Tradeoff in Mobile Platforms

Both QoS and Security are needed in mobile platforms, and the tradeoff is present at different levels:

- New capabilities developed for commercial purposes. For example, *Near Field Communication* (NFC) provides built-on security technology but can also increase the transmission time due the cryptographic mechanisms. Moreover, QR-code may be used as the Authentication token decreasing the response time in the authentication step.
- Development of new software. For example, Inheritance-based mechanisms complicate the privacy mechanisms (e.g. space randomization) because inheritance enables shared memory between related processes.
- Communication network. Security mechanisms consume network resources in order to work. For example, the peer authentication increases the data transmission and therefore the power consumption.

Note that, Security and QoS tradeoff affects user's experience, which is fundamental for the platform's survival. For example, the authentication based on keystroke mechanisms may improve user's experience in the system because it avoids security mechanisms dependent on the user's memory (e.g. passwords) or on tokens [8]. However, it can also degrade user's experience if the new techniques notably increase power consumption or require excessive memory space in order to work.

Traditional QoS mechanisms (e.g. QoS signaling) are also a problem in that respect because data transmission leads to greater power consumption [9] [10], but it may also improve the user's experience by managing the network resources in order to provide, for example, streaming services or any other service which increases the functionality of the mobile device.

Indeed, popular mechanisms such as QR-code and NFC have been developed to increase the functionality of mobile phones and therefore increase user's experience. Specifically, although QR-code can be used to

decrease the response time for security services implementing authentication based on tokens [11], it is exposed to attacks if it is combined with other techniques or social engineering [12] [13]. Furthermore, NFC provides built-in cryptographic mechanisms; thus, mobile payment and signalling become possible using this technology. It appears to be like the *Trusted Platform Module* (TPM)[1] but in a mobile platform environment, and this is very interesting from a security point of view, althought it has been demonstrated that this type of mechanism increases the transmission time [14]. The user usually trusts these new technologies, despite the security flaws [15] [16] [17] [18], but they can stop using them if in the end the new mechanisms developed to use these new technologies affects the performance.

In fact, challenges to satisfy new market demands concentrate on improving QoE, which considers QoS parameters and the user's experience. However, with a growing number of attacks, users are starting to consider exactly what happens with their data. Thus, privacy is a mayor issue in mobile platforms that also has to be considered in the development of new technologies, either for random allocation of private data (e.g. *Address Space Layout Randomization* (ASLR)) or to remotely wipe data if a mobile phone has been stolen. Regarding this, the way data is deleted from the mobile phone is very important since it has been shown that it is possible to recover residual data from mobile phones even after it has been deleted [19].

Another point to consider is how it is possible to improve the capabilities of mobile devices in order to enhance the end-to-end QoS without damaging the device's performance at low level. In that regard, several studies have focused their attention on the use of multiple radio antennas and *Multiple-input and Multiple-output* (MIMO) technology. In fact, the use of multiple radios allows better transmission services at higher speeds and also offers the possibility for early detection of collisions, among other things. However, in order for this technology to be able to offer these improvements it has to consume a lot more battery and other resources in the device. The extra battery drain may occur during the handover process or because the use of multiple interfaces, where, in general, the handover process is powerful [20]. Also the concurrency due to multiple protocols increases the complexity of the mobile devices and may cause interference. In particular, noise is one factor which certainly leads to performance degradation [21], and therefore results in a poor QoE.

Note that problems are compounded where there is a necessary increase in the functionality of personal devices attempting to satisfy the user, in order to promote the use of new technologies. As a consequence, today's mobile platforms are multimedia devices enabled to provide different types of traffic with the consequent and special performance demands and, of course, security needs.

[1] http://www.trustedcomputinggroup.org

1.3 Document Structure

The rest of the paper is structured as follows. In Section 2 the main *action layers and parameters* identified in mobile platforms are described. Section 3 presents the Parametric Relationship Model (PRM) which will be used in Sections 4 and 5 to perform the analysis of the Security and QoS tradeoff. Specifically, Section 4 explains how a mobile system can be defined according to the PRM defined in Section 3. In Section 5, the results based on the modelled system are analysed. Finally, Section 6 discusses our conclusions.

2 Action Layers in Mobile Platforms

As stated, our main goal is to analyse the Security and QoS tradeoff in mobile platforms. To accomplish this, we should perform an analysis based on a set of parameters which define the environment appropriately. This is not an easy task because, although extensive literature exists about challenges in mobile platforms environments, the work has mainly focused on solving specific problems or showing an overview of concepts within a particular area. This helps to simplify the problem so that it can be locally solved, without considering the whole environment. However, it gives us only a piece of the puzzle to be solved.

In order to analyze the parameters together (giving us more information about the system) while reducing the complexity and, therefore, increase the usefulness of this work, we consider that the parameters should be classified in different layers, named *Action Layers*. In particular, we decompose into five main action layers, according to the location of the parameters in a given mobile scenario: High-Level Requirements, Local Properties, Communication, Measurements and Environment. Table 1 shows the complete list of parameters used throughout the analysis and the level they are assigned to.

2.1 Cross-Layer Relationships

Before starting with the description of the levels, it is important to point out that in this paper it is assumed that any parameter at any layer may be related with

HIGH-LEVEL REQUIREMENTS	
SLA traffic classes	Streaming, interactive, conversational, background
Performance	Reliability, availability, fault tolerance
Security	Authentication, authorization, confidentiality, integrity, non-repudiation, trust, privacy, accounting
Attacks	Social engineering
QoE	QoS traffic classes, user's experience (UX)
MOBILE PLATFORM (LOCAL PROPERTIES)	
Resources	Power consumption, allowable memory
Characteristics	Context-based behaviour, inheritance, concurrency, location, NFC, QR-code
Security	Space randomization, anti-tampering, encryption, public key cryptography, symmetric cryptography, secure key exchange, secure key redistribution, key generation
Attacks	Break-in
COMMUNICATION	
QoS Parameters	Data rate, packet size, signal strength, data transmission, transmission time, transmission power
Characteristics	Time-sleeping, required time-on, multiple antennas, buffering
Attacks	Tracking, eavesdropping, injection
Consequence	Retransmmission
MEASUREMENTS	
QoS Parameters	RTT, throughput, delay, jitter, packet loss, response time, BER
ENVIRONMENT	
Performance	Handover time, allowable bandwidth, error probability
Characteristics	QoS signaling, mobility support
Attacks	DoS, Malicious devices
Consequence	Interference, congestion, overhead, fading, shadowing, noise

Table 1 Action Layers and Parameters considered

any other parameter at any other layer. Therefore the difference is per type of parameter rather than per functionality. For example, if the response time is taken as one parameter at Measurement layer, then it will be also related with the High-Level Requirements layer.

Intuitively, while more parameters are considered at each layer, less cross-layer dependability may occur because the cross-layer parameters set could be limited better. For example, if certain authentication mechanisms were introduced into the model (as Local Properties at the Mobile Platform layer), then relating the response time with the authentication requirement based on these mechanims may be possible. Thus, the model could become richer and more specific. However, it would be more complex too. So, we have decided to maintain some direct dependencies (cross-layer dependencies) among different layers to simplify some relationships.

2.2 High-Level Requirements

The first layer takes into account *High-Level Requirements* (HLR), that is, concepts usually understandable by the users or software developers. Security requirements and QoS types of traffic are defined at this layer. Moreover, at this level, QoE requirements should be considered in order to evaluate the impact of requirements on the user's experience/satisfaction[2].

Basic Security Requirements considered are:

- Authentication. The ability to ensure that an entity or user is who they say. This property has to be provided not only between the user and the mobile platform infrastructure and viceversa, but also among users.
- Authorization. The ability to access one or more services offered by the network. In mobile platforms this depends on the SP infrastructure.
- Confidentiality. The ability to ensure that the data is only accesible by authorized entities or users in the network. It can be related with the use of personal data and its maintenance according to the law. Confidentiality depends on the SP, but can be affected by the security mechanisms implemented at the low layer.
- Integrity. The ability to ensure that the data is not modified by any non-authorized third party in the network. It depends on the SP infrastructure but also on the mobile terminal.
- Non repudiation. The ability to ensure that no entity or user can lie about its actions over the environment. In mobile platforms it depends on the SP infrastructure and the authentication, authorization and accounting capabilities.

[2] Note that the user's experience is a very subjective parameter, because it depends on the user's opinion, which is based on their personal experiences.

- Privacy. It can be addressed from various points of view: user's data privacy in general (data stored by the mobile network infrastructure, depending on the SP), personal data stored in the mobile phone and data collected by network applications for business purposes. Privacy is related to the right of any user to decide how their data is used.
- Accounting. The ability to store relevant information about the user's participation in the network. In mobile platforms it depends on the SP infrastructure.
- Trust. The relationship between two or more entities or users based on reputation. It is essential in order to guarantee both the future use and maintenance of current mobile platforms. Trust is a parameter very much related with the user's experience and therefore with business objectives.

Moreover, basic QoS traffic classes considered are: streaming, Interactive, Conversational and Background, that corresponds to the UMTS Service-Level Agreement (SLA) Traffic Classes according to [4]. Furthermore, there are high-level requirements usually related with the performance that we have to consider at this level:

- Reliability. Measures the capability of the system to work properly.
- Availability. Measures the capability of the system in order to offer the user/services the resource or services requested.
- Fault Tolerance. Is the ability of the system to be operative (resist) after a fault or incident. For example, this property can be implemented by using redundant equipment.

2.3 Mobile Platform (Local Properties)

Local properties are located in the mobile environment. So, hardware improvements such as multiple antennas, NFC or any additional device can be considered as part of it. However, keeping a certain simplicity, those elements used to interact with the network are set in the Communication layer. Thus, Local Properties here are closest to the independent-network properties.

For example, power consumption is extremely dependent on network transmission. However, it is also affected even when not connected to any network. The same thing is true for the allowable memory parameter.

The parameters in this layer depend on the implementation of the mechanisms and applications deployed and on the mobile equipment built on the device by the manufacturer.

2.4 Communication

The set of parameters that are considered as part of this layer are related with the communication of the node with the network. For example, the data rate parameter defines the number of bytes sent per unit of time (also named Bit Rate). Therefore, this parameter is closely related with data transmission and packet size, because the less data to be sent, the less time the system dedicates to send the data. As a consequence, data transmission is also considered in this layer. It is supposed that security mechanisms have been applied in previous layers; thus, in this layer, encrypted data may be received to be sent, but there are no security mechanisms to manage the data. This layer is composed by:

- Resources and measurements of the local interfaces. For example: packet size or signal strength.
- Characteristics and elements that can be used at this layer. For example, the time that the interface is on (the required time that it has to be listening) or innactive (out of service or sleeping).
- Attacks related with the interface. Indeed, these attacks can be considered in the environment layer in the case they are considered to be threats only present in the environment. The *Communication* layer shows that the wireless capabilities provide the opportunity for these threats.
- Consequences due to poor quality in the communication, for example, the retransmission of the data.

2.5 Measurements

This layer is used to take performance measurements related with the network. At this layer, typical parameters to measure the network performance are used:

- Throughput. The amount of data that the system can deliver per user. This parameter shows the real volume of traffic that may be sent through the network, and therefore the current needs.
- Delay. The time elapsed since the data is sent from the source until it arrives to its destination[3].
- Jitter. The difference between consecutive Delays. This parameter shows the stability of the network.
- Packet Loss. The volume of packets which were sent from the source but didn't arrive at their destination.

[3] Note that in (10) the equation is simplified in order to show the example. Indeed, in (10) the data rate parameter may be considered as the time which the network consumes to deliver the data end-to-end, although in this analysis we consider data rate as one parameter measured at the Communication layer.

- Response Time. Is the time taken by one system or application to respond to another system, application or user.
- Round Trip delay Time (RTT). The time spent to send data to one destination and receive the response, considering only the time expended in the transmission of the data.
- Bit Error Rate (BER). Percentage of wrong bits recived at the destination (total number of bits received divided by the wrong bits).

2.6 Environment

Finally, in the Environment layer the parameters related with network conditions and characteristics of the environment are considered. For example, the place where the user is, at a given time, does not support handover properties (or is supported but not for a particular service or user).

In fact, the environment defines the scenario and the current context where the mobile device is. So, it is precisely this layer that is expected to change the most throughout the lifetime of the device.

Similarly, the environment is affected in some way by the presence of the mobile device. Thus, the objective of defining this layer is twofold. On the one hand, it is useful from a context viewpoint. If the environment changes, the performance and therefore the value of the QoS parameters may vary in the whole device. On the other hand, from the point of view of service providers and network administrators it is important to measure the impact that one device has on the parameters of the environment. In particular, this layer also considers the consequences related with networking conditions. For example:

- Interference. Anything affecting the signal by modifying it or difficulting the decoding of the original signal on the receptor side. For example, this could occur when two devices try to send data using the same channel at the same time.
- Fading. The deviation of the attenuation and is very dependent on the distance between the emisor of the signal and the receptor.
- Shadowing. It is the deviation of the attenuation caused by physical obstacles in the environment.
- Noise. Anything that affects the propagation medium, in this case, the wireless medium. It may be caused by many factors, including environmental conditions.
- Congestion. A network state that is reached when the system cannot properly deliver the data. It happens because of inadecuate utilization of network resources or under network attack conditions.
- Overhead. A network state in which the system delivers more data than expected and with no more resources to cope [4].

3 Parametric Relationship Model (PRM)

In this section we present the *Parametric Relationship Model* (PRM) which defines the dependencies among parameters in a mobile platform environment. The PRM is defined in order to take into account the influence of one parameter on the rest of parameters considered.

3.1 Mathematical Definition

The PRM used to define the relationships between the parameters was proposed in [7] and is shown in Table 3.1. It is composed by the *Basic Formulation Set* (BFS,1-4) and the *Complex Formulation Set* (CFS, 5-9).

Basic Formulation Set	
$D^{+} :: aD^{+}b \Rightarrow (\Delta a \rightarrow \Delta b)$	(1)
$D^{-} :: aD^{-}b \Rightarrow (\Delta a \rightarrow \nabla b)$	(2)
$D^{\neg +} :: aD^{\neg +}b \Rightarrow (\nabla a \rightarrow \nabla b)$	(3)
$D^{\neg -} :: aD^{\neg -}b \Rightarrow (\nabla a \rightarrow \Delta b)$	(4)
Complex Formulation Set (based on 1-4)	
$D^{c} :: (\Delta a \rightarrow \Delta b) \wedge (\nabla a \rightarrow \nabla b) \equiv aD^{+}b \wedge aD^{\neg +}b$	(5)
$D^{t} :: aD^{c}b \wedge bD^{c}a$	(6)
$D^{\neg c} :: (\Delta a \rightarrow \nabla b) \wedge (\nabla a \rightarrow \Delta b) \equiv aD^{-}b \wedge aD^{\neg -}b$	(7)
$D^{i+} :: (\Delta a \rightarrow \Delta b) \wedge (\nabla a \rightarrow \Delta b) \equiv aD^{+}b \wedge aD^{\neg -}b$	(8)
$D^{i-} :: (\Delta a \rightarrow \nabla b) \wedge (\nabla a \rightarrow \nabla b) \equiv aD^{-}b \wedge aD^{\neg +}b$	(9)

Table 2 Parametric Relationship Model (PRM)

The BFS (1-4) is defined in order to get a basic set of equations from which any relationship can be derived. Responsible for observing the behaviour of the system when the parameters increase or decreasse (or when the requirements are provided or not), the BFS is composed of the following relationships:

- Positive $(D^{+}, 1)$. The increment of the first parameter also causes an increment of the second parameter.
- Negative $(D^{-}, 2)$. The increment of the first parameter causes the decrement of the second parameter
- Inverse positive $(D^{\neg +}, 3)$.The decrement of the first parameter causes the decrement of the second parameter.
- Inverse negative $(D^{\neg -}, 4)$.The decrement of the first parameter causes the increment of the second parameter

[4] Note that the overhead property may also be calculated for a particular node.

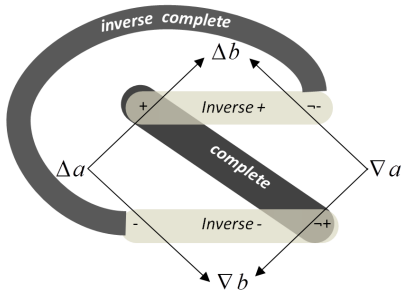


Fig. 1 PRM Diagram

CFS (5-9) is defined in order to simplify the dependency relationships diagrams based on the PRM. The equations in CFS are defined as follows:

- Complete ($D^c, 5$). The action (increase/decrease) to be applied on the second parameter is the same as in the first parameter.
- Total ($D^t, 6$). Both parameters are related with a complete relationship.
- Inverse complete ($D^{\neg c}, 7$). The action (increase/ decrease) to be applied on the second parameter is the opposite to that in the first parameter.
- Independent positive ($D^{i+}, 8$). If the first parameter changes, then the second paramaeter will always increase, regardless the type of value change in the first parameter.
- Independent negative ($D^{i-}, 9$). If the first parameter changes, then the second paramaeter will always decrease, regardless the type of value change in the first parameter.

Figure 1 shows the relationship between the definitions in Table 3.1. Note that the *total* relationship occurs when the complete relationship between a and b is symmetric.

3.2 Examples

For example, given the Equations (10-13), we extract the dependencies (14-20) shown in Table 3[5].

$$Delay = \#bits/DataRate \quad (10)$$
$$Jitter = |DelayTo - DelayT1| \quad (11)$$
$$Throughput(peruser) = DataRate/\#Users \quad (12)$$
$$TransmissionTime = PacketSize/BitRate \quad (13)$$

[5] The difference between bit rate and data rate is basically the quantification, respectively, bits per second (bps) and bytes per second (kB/s). So, in the following we use Data Rate.

Delay, jitter and throughput are parameters considered at low level. These parameters are related with the performance in communication networks, but there are other parameters working at different levels which can be considered, depending on the system and the tradeoffs to be analysed.

4 Mobile System based on PRM

The decomposition in different levels not only allows us to properly define the relationships among parameters, the requirements and characteristics within the same level but also between different levels in a simplified way. The system becomes really complex when putting all the parameters together. Thus, in order to minimize the computation time, we decompose the problem into one layer-based problem, as Table 1 shows. Table 1 also shows the parameters that are considered at each level.

Throughout the analysis, seven types of parameters are considered:

- Traffic classes and Performance parameters. Traffic classes are defined based on the UMTS SLA traffic classification [4]. These parameters are directly related with performance parameters at low level, which are named QoS parameters. The traffic classification is part of the QoS engine, and, in particular SLA traffic classes are internally translated to QoS performance requirements. The SLA traffic classes are closer to the user's language than the QoS performance parameters, and can be mapped to the *Mean Opinion Score* (MOS) that is understood by the users, and therefore used to measure the user's opinion.
- The QoE considers the user's experience/opinion and the QoS. In this paper, the QoS is considered as one QoE parameter, that is a high-layer metric.
- The characteristics of one platform are logical improvements that can be present in a platform or not. They are mostly high-layer parameters.
- Security requirements and mechanisms focus on the two first layers (high-level requirements and local properties). This is because requirements are needed at high-level, understood by users or services. Moreover, they may also be present in the mobile device as part of the built-on security suite.
- Attacks may occur at different layers, but in this work they are considered only as one more indication of possible risks.
- Consequences due to the influence of the parameters in the system.

In the following we analyze each level showing the relative PRM diagram, emphasizing the Security and

Example using Delay (10)	
$(\Delta DataRate \rightarrow \nabla Delay) \wedge (\nabla DataRate \rightarrow \Delta Delay) \equiv DataRateD^{c}Delay$	(14)
$(\Delta \#bits \rightarrow \Delta Delay) \wedge (\nabla \#bits \rightarrow \nabla Delay) \equiv PacketSizeD^{c}Delay$	(15)
Example using Jitter (11)	
$(\Delta Delay \rightarrow \Delta Jitter) \wedge (\nabla Delay \rightarrow \Delta Jitter) \equiv DelayD^{i+}Jitter$	(16)
Example using Throughput (12)	
$(\Delta DataRate \rightarrow \Delta Throughput) \wedge (\nabla DataRate \rightarrow \nabla Throughput \equiv DataRateD^{c}Throughput$	(17)
$(\Delta \#Users \rightarrow \nabla Throughput) \wedge (\nabla \#Users \rightarrow \Delta Throughput) \equiv \#UsersD^{c}Throughput$	(18)
Example using Transmission Time (13)	
$(\Delta BitRate \rightarrow \nabla TransmissionTime) \wedge (\nabla BitRate \rightarrow \Delta TransmissionTime) \equiv BitRateD^{c}TransmissionTime$	(19)
$(\Delta PacketSize \rightarrow \Delta TransmissionTime) \wedge (\nabla PacketSize \rightarrow \nabla TransmissionTime) \equiv PacketSizeD^{c}TransmissionTime$	(20)

Table 3 Using the defined model to derive relationships

QoS tradeoff. Finally we show the results of the analysis. The dependency diagrams are defined based on the PRM, implemented using the DOT language[6] and interpreted using MATLAB.

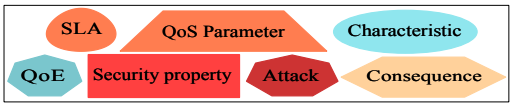


Fig. 2 Legend for Figures 3,4,5,6 and 7

4.1 High-Level Requirements

Parametric relationships focus on the HLR Layer are shown in Figure 3. In this first diagram, it is possible to observe the dependencies chain. In particular, security requirements are taken into account in this layer because it is close to the service requirements and user needs. Specifically, both security requirements and QoS traffic classes affect the user's experience. Note that, in this layer, low-level QoS parameters (e.g. delay) are not taken into account, so if the security requirements are provided, apparently the user's experience only increases.

Moreover, there are no characteristics. Instead, the HLR layer defines closer-service requirements that may affect the Environment characteristics. Of course, if the response time is taken as one Measurement, it is also related with the HLR layer.

The relationships with the HLR parameters in the Mobile Platform layer are shown in Figure 4. Note that Trust can be considered as a parameter that influences the user's experience, because if the system is not trustworthy and the user considers this to be the case, then the experience becomes poor. Trust can be a addressed as the union of reliability and security properties.

[6] www.graphviz.org

4.2 Mobile Platform (Local Properties)

Figure 4 also shows the parametric relationships related with this layer based on the PRM. In this layer the objective is to provide mechanisms that enforce high-layer requirements related with security and to ensure the QoS.

For this layer, security mechanisms, characteristics and local resources (e.g. memory) are considered. In this case, note that the Mobile Platform layer is related with the Communication layer in order to be used by some mechanism or to satisfy some security property (e.g. secure key exchange).

In this paper, only power consumption and allowable memory have been considered as local parameters. Moreover, the allowable memory is defined in general terms, taking into account the memory of the user's applications and the memory at low level (e.g. buffer). However, it is possible to increase the number of parameters to be considered (e.g. time processing).

Note that security mechanisms are taken into account at this layer, and not in the Communication, Measurement or Environment layers. This is very important because nowadays security mechanisms depend on the Mobile Platform. The only additional layer where security could be considered is the Environment layer, where Intrusion Detection Mechanisms could be taken into account, for example, in order to stop *Denial of Service* (DoS) attacks. However, these types of mechanisms are beyond the scope of the work here.

Furthermore, in the Communication layer, only the parameters related with the wireless interface are considered, and, in the Measurements layer, the QoS parameters used to evaluate the network performance are analysed. This is the reason why the following two layers do not consider security requirements or mechanisms.

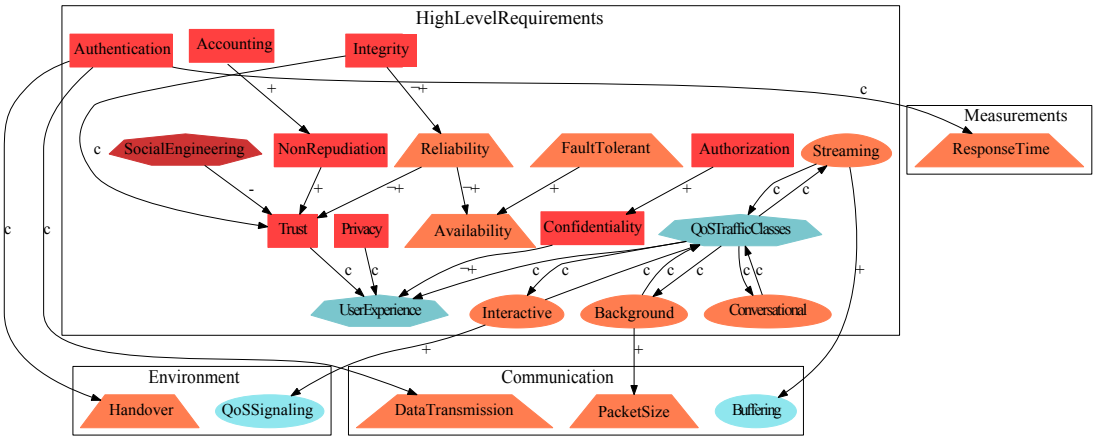


Fig. 3 High-Level Requirements based on PRM

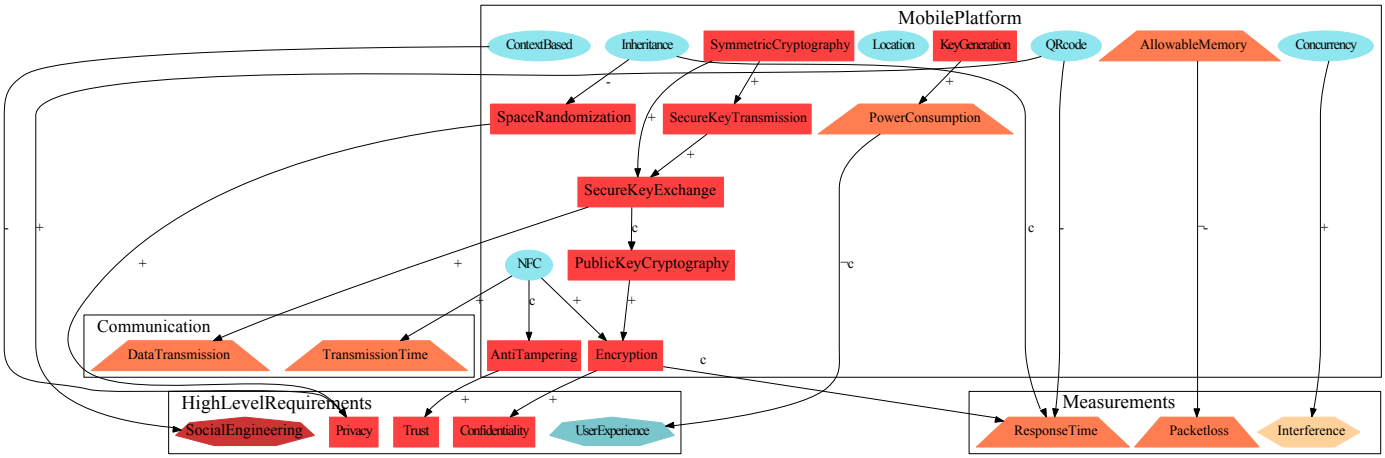


Fig. 4 Local Properties based on PRM

4.3 Communication

Figure 5 shows the parametric relationships related to this layer based on the PRM. In particular, in this layer the local resources memory and power consumption are considered. In fact, the impact that wireless interfaces can have on the second one is well known. Intuitively, the measurements over the environment are influenced by the actions performed in the Communication layer.

Furthermore, the formulation in Table 3 is shown in both Communication and Measurements layers. Also intuitively, the decisions taken in the Communication layer can affect the measurements of the system.

4.4 Measurements

Figure 6 illustrates the parametric relationships in the Measurements layer based on the PRM. In particular, delay, jitter and packet loss are typical parameters for measuring the network's performance. In mobile platforms, it is also important to pay close attention to the response time and those parameters directly related to the type of service that a mobile platform is expected to offer satisfactorily.

The relationships with the parameters in the HLR are very interesting because it provides feedback on the network utilization. In fact, the type of traffic (SLA traffic classes) is highly dependent on the network performance and, in particular, on the QoS parameters considered in this layer.

Figure 6 shows that when a parameter affects any of the QoS parameters defined here, then the *SLA traffic classes* can also be affected, and so too the user's experience.

4.5 Environment

In the Environment layer, shown in Figure 7, the parameters of type Consequence are highlighted, because

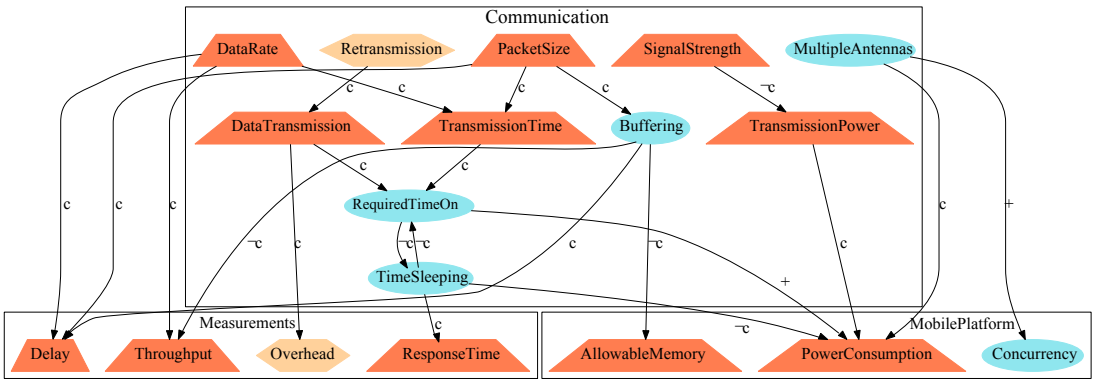


Fig. 5 Communnication properties based on PRM

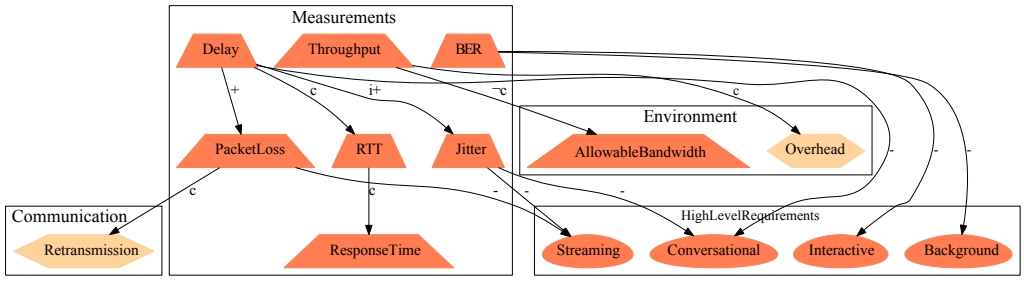


Fig. 6 Measurements based on PRM

this layer represents the impredictability of the context where the user is.

Moreover, the Environment parameters are closely related to the Measurements parameters. It is intuitive because the objective of the Measurement parameters is to show the network conditions in order to prove that the QoS requirements defined in the high-layer are satisfied. In other words, by changing the parametric relationships (or the value of these) in the Environment layer according to one particular context, it is possible to get different measurements based on the context.

In addition, the presence of malicious devices or the influence of attacks such as DoS or the QoS signaling attack may be considered in this layer. In such cases, HLR as the availability or trust may be affected. Note that the QoS signaling is one characteristic which allows resource reservation along the path. However, these types of mechanisms can also be used by malicious devices in order to perform DoS attacks.

5 Analysis based on Inter-Layer Results: Security and QoS tradeoff

PRM provides relevant data on a system once we have defined the parameters of the system accordingly. In particular, it is possible to extract the following information:

1. Influence on a parameter Y, $X \rightarrow Y$ (or on a set of parameters).
2. Dependence on a parameter X, $X \rightarrow Y$ (or on a set of parameters).
3. Impact on the system when a parameter (or a set of parameters) increases or decreases its value, or when a requirement is provided or not.

Figure 8 shows the acumulative influence (ι) and acumulative dependence (δ) based on the parameters considered in Table 1. ι and δ are calculated based on Equations (21) and (22) respectively, for a generic parameter a which belongs to the set of parameters P defined in the PRM, as follows:

$$\iota(a) = |I_a| = |\{x | x \rightarrow a \vee xRa, x \neq a, x \in P\}| \quad (21)$$

$$\delta(a) = |D_a| = |\{y | a \rightarrow y \vee aRy, y \neq a, y \in P\}| \quad (22)$$

$$xRy \iff x \rightarrow y \vee \exists k | k \in D_x \wedge k \in I_y \quad (23)$$

5.1 Acumulative Influence

The acumulative influence on a parameter Y (Eq. 21) reflects how many parameters X can affect the param-

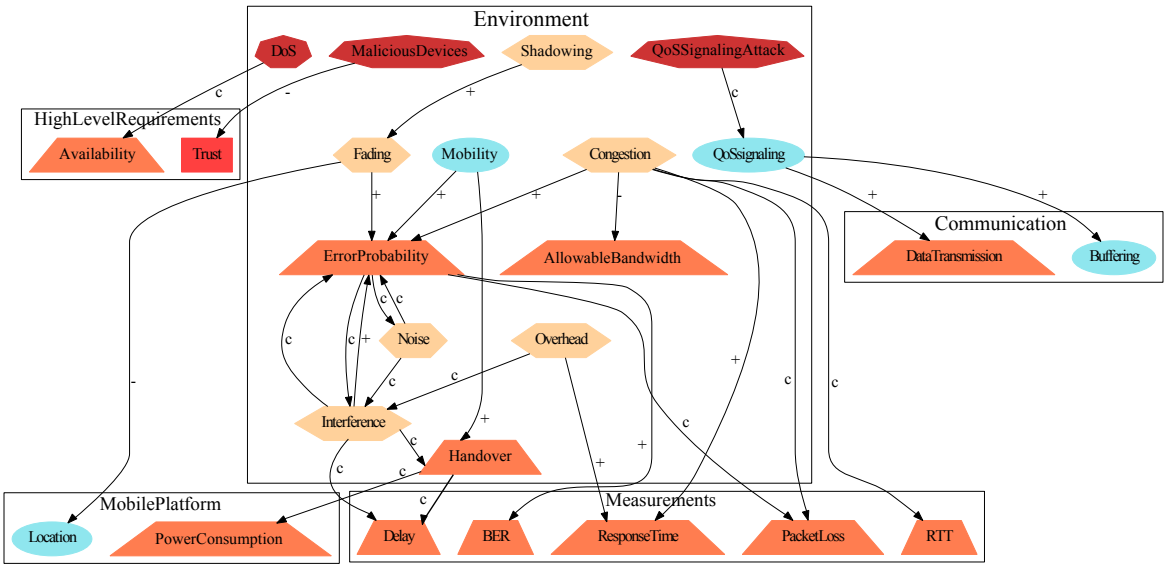


Fig. 7 Environment based on PRM

eter directly ($X \rightarrow Y$) or indirectly through another parameter ($X \rightarrow ... \rightarrow Y$). In other words, in Figure 8 the parameters with values up to zero are affected by the rest of the parameters and the parameters with values equal to zero are not affected in the diagrams considered. According to Figure 8(a), the QoS parameters are highly influenced by the rest of the parameters of the modeled system. In fact, they are influenced by nearly fifty percent of the parameters, characteristics and requirements considered [7].

It is especially important to highlight that the power consumption and the response time parameters are the most influenced parameters in this scheme, followed by the characteristics that in the Communication level describe the use of the antennas (e.g. required time on). This is logical, because the acumulative influence highlights those elements which in the end can be affected by the rest of elements.

For example, according to Figure 8(a) the user's experience may be influenced by the rest of the parameters. However, the user's experience value is not present in Figure 8(b), because in our scheme the user cannot take part in the system to modify the system's behaviour. However it is possible to intuit what can affect his/her perception from a business and usability point of view. So, in our scheme it is possible to influence the user's opinion but without them being able to do anything about it.

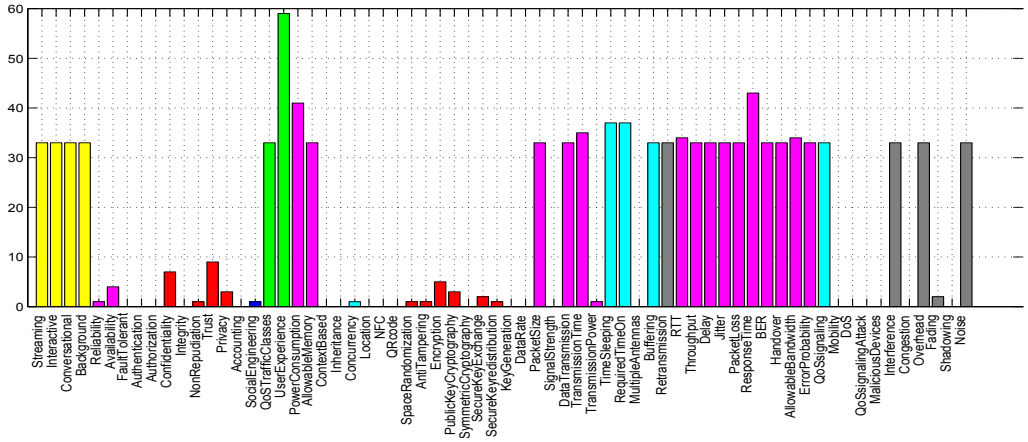
[7] In total around seventy six parameters are considered.

5.2 Acumulative Dependence

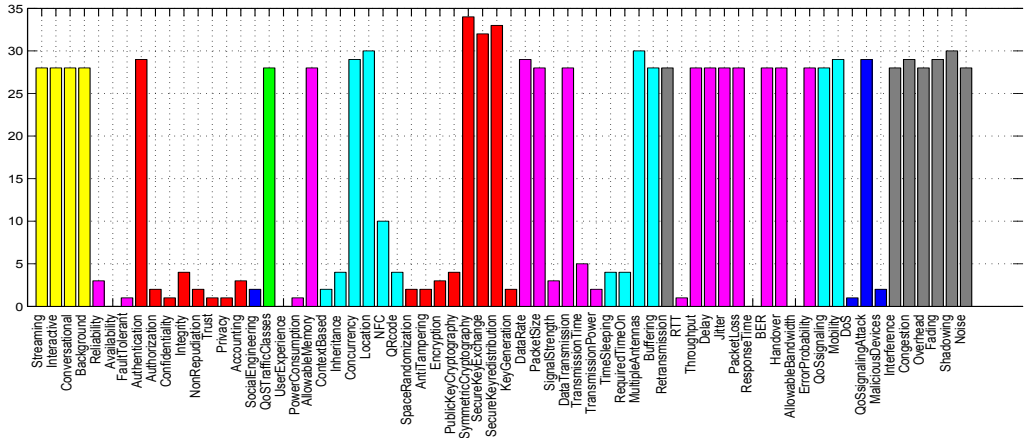
The acumulative dependence (or dependence degree) on a parameter X (Eq. 22) reflects how many parameters Y are affected if the value of X changes (directly or indirectly through others parameters). The difference by type of parameter is not as remarkable as in the previous case. So, it is important to highlight one detail about how the measurements are taken. The values shown in Figures 8-9 are measured taking into account the formulation in Table 3.1, which does not consider weights on the links. This is because the weight should be set depending on the scenario being considered and will vary according to the current context where the user is. It is one interesting question but is beyond the scope of this work.

For example, according to Figure 8(b), the acumulative dependability value on trust is very low. However, this should not be misunderstood; in one insecure system of social environment this requirement could be very important. Moreover, security mechanisms as the symmetric key cryptography or the requirement for a secure key exchange plays important roles in said figure due to their impact on a large chain of performance measurements and requirements.

Regardless, note that even in a system where the links are marked with weights the number of relationships and acumulative dependability do not change. And, of course the system depends on the environmental conditions, security mechanisms, characteristics, and performance.



(a) Acumulative Influence on Y, $X \rightarrow Y$



(b) Acumulative Dependence on X, $X \rightarrow Y$

Fig. 8 Inter-Layer results

5.3 Impact of Security Requirements on the QoS Parameters

Finally, using the model it is also possible to get data about the positive or negative influence which a parameter or a set of parameters can have on the rest. The impact of a parameter x on another parameter y, is measured according the Equations (24-25).

The value of a parameter x (given by $v(x)$) is increased (Δ) or decreased (∇). When it happens, the system updates the values for the rest of parameters related with x. The updating process is provided in Equation (24-26), and depends on the operation performed on the antecedent on the relationship R defined betweeen the parameter x (antecedent) and the rest of parameters (consequents). The value of one relationship is given according with Ω, defined in Table 4.

Ω is defined based on Table 3.1. Therefore, Ω decides if, given a relationship defined in the PRM (R), the parameter in the consequent have to be increased

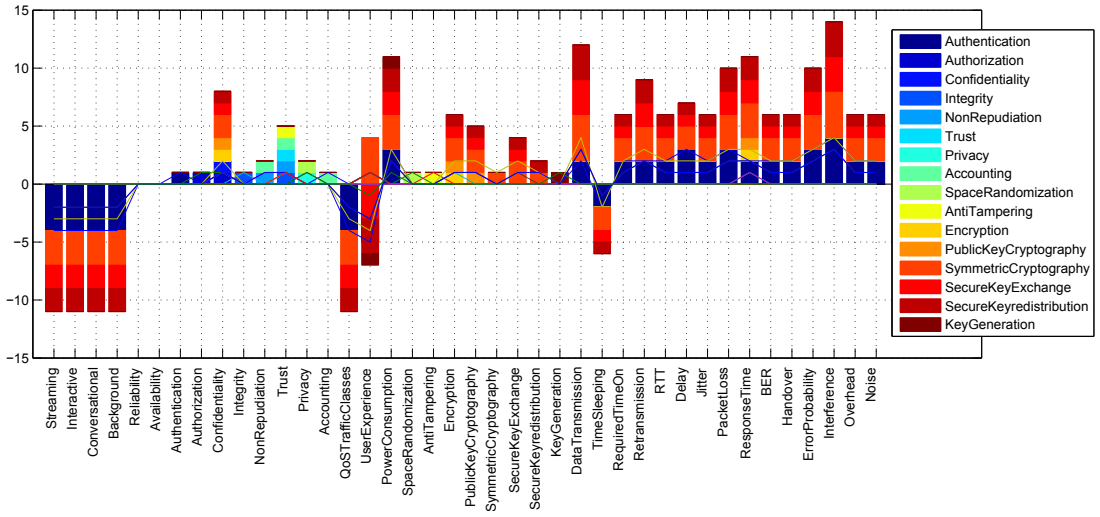
$$\Delta x \implies \forall y | xRy, v(y) = v(y) + \Omega(R, \Delta x) \wedge u(y, \Omega(R, \Delta x)) \quad (24)$$

$$\nabla x \implies \forall y | xRy, v(y) = v(y) + \Omega(R, \nabla x) \wedge u(y, \Omega(R, \nabla x)) \quad (25)$$

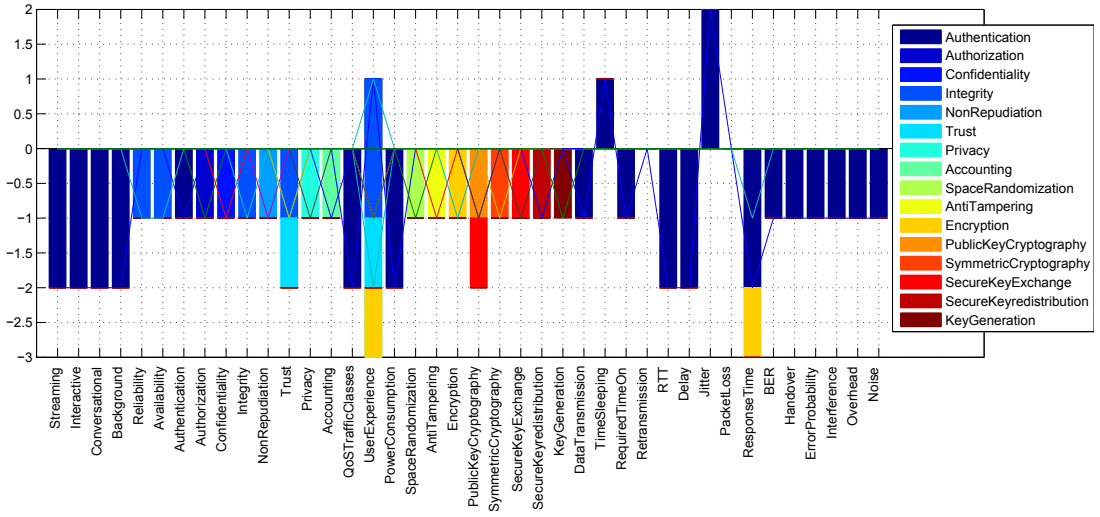
$$u(x, \omega) = \begin{cases} \Delta x \text{ if } \omega > 0; \\ \nabla x \text{ if } \omega < 0; \end{cases} \quad (26)$$

R	Operation on x	
(Symbol)	Increase x (Δx)	Decrease x (∇x)
$+$	$+\omega(+, a)$	NTD
$-$	$-\omega(-, a)$	NTD
$\neg+$	NTD	$-\omega(\neg+, a)$
$\neg-$	NTD	$+\omega(\neg-, a)$
c	$+\omega(c, a)$	$-\omega(c, a)$
t	$+\omega(t, a)$	$-\omega(t, a)$
$\neg c$	$-\omega(c, a)$	$+\omega(\neg c, a)$
$i+$	$+\omega(i+, a)$	$+\omega(i+, a)$
$i-$	$-\omega(i-, a)$	$-\omega(i-, a)$

Table 4 $\Omega(R, x)$



(a) Providing Security Requirements



(b) Retrieving Security

Fig. 9 Influence of Security on the System

or decreased, or instead there is nothing to do (NTD, value 0 in the current model)[8]. Therefore, In general, the value in $\Omega(R, x)$ is given based on a weight ω that depends on R, but also can depends on x. Note that, $\omega(R, x)$ defines the weight that the parameter x has on the relationship. In this paper, ω is equal to 1 for all the relationships and parameters. The variation of this parameter would provide different contexts and ways of interpreting the information. However, it would require several testing proofs and lead beyond the scope of this work to describe this process in detail.

For example, Figure 9(a) shows the negative impact that security mechanisms have on network performance and therefore on the QoS parameters. Note that this behaviour decreases but also increases the user's experience. This is because in our model the security requirements enhance the user's opinion about the system, because he feels safer. However, the performance degradation can not be ignored, even more so when the power consumption is vastly increased according to the model. Again, in a context where the links were marked with weights, this behaviour should be modified based on the importance to the system of QoS traffic classes against security requirements. This could vary based on the context where the user is (at home or walking around).

Moreover, in Figure 9(b), we can see two main points: first, it has to be noted that the user's experience in-

[8] For example, if aD^+b and ∇a, then the value of b is not modified, because b is only affected when a increases.

creases and also decreases as in Figure 9(a). This is because in that case the overhead caused by the security mechanisms is not present. Moreover, the only negative influence on performance is that the jitter increases, but only because the delay is fluctuating[9].

However, the user's experience decreases because the environment is not secure and the user may have noticed. This situation is highly dependent on the context and also on the user. Once again, the user's opinion about the security parameter is very subjective.

6 Conclusions

In this paper the Parametric Relationship Model (PRM) defined in our previous paper [7], has been used to analyse the Security and QoS tradeoff in mobile platforms. The analysis has been carried out based on the interdependencies in one large parameters set. In this type of scenario, the problem becomes really complex, and for this reason we suggest a decomposition into five contextual layers in order to properly define the relationships between parameters, requirements and characteristics not only within the same layer but also between different layers, in a simplified way. Once the dependencies on mobile platforms has been defined according with the PRM the analysis shows relevant characteristics of the system. Note that the current proposal has two main issues to be discussed. On the one hand, the current PRM does not consider different weights in the relationships between parameters. Thus, it does not allow different interpretations of the same diagram. For example, it would be desirable that in some contexts the parameter Trust increased in relevance (e.g. outside the home environment), and this is not currently possible. On the other hand, the boundary of the solution depends greatly on the parameters set considered. It is very intuitive. Thus, the more parameters, the more complex the system but also the more information about the dependencies it provides. In this paper the parametric relationships are based on the current literature on mobile platforms but it could easily be increased.

7 Acknowledgment

This work has been partially supported by the Spanish Ministry of Economy and Competitiveness through the projects ARES (CSD2007-00004) and SPRINT (TIN2009-09237), being the last also co-funded by FEDER. Additionally, it has been funded by Junta de Andalucia through the project FISICCO (TIC-07223). The first author has been funded by the Spanish FPI Research Programme.

[9] The jitter is increased because the delay is continuously decreasing while the test. Once the delay is stable, then jitter remains stable too.

References

1. M. La Polla, F. Martinelli, D. Sgandurra, *A Survey on Security for Mobile Devices*, Communications Surveys Tutorials, IEEE **15**(1), 446 (2013). DOI 10.1109/SURV.2012.013012.00028
2. A. Hoog, K. Strzempka, *IPhone and IOS Forensics: Investigation, Analysis and Mobile Security for Apple IPhone, IPad and IOS Devices* (Syngress, 2011)
3. G. Delac, M. Silic, J. Krolo, *Emerging security threats for mobile platforms*, in *MIPRO, 2011 Proceedings of the 34th International Convention* (2011), pp. 1468 –1473
4. S. Mohan, N. Agarwal, *A convergent framework for QoS-driven social media content delivery over mobile networks*, in *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on* (IEEE, 2011), pp. 1–7
5. C. Lorentzen, M. Fiedler, H. Johnson, J. Shaikh, I. Jorstad, *On user perception of web login - A study on QoE in the context of security*, in *Telecommunication Networks and Applications Conference (ATNAC), 2010 Australasian* (2010), pp. 84 –89. DOI 10.1109/ATNAC.2010.5680262
6. K. De Moor, I. Ketyko, W. Joseph, T. Deryckere, L. De Marez, L. Martens, G. Verleye, *Proposed framework for evaluating quality of experience in a mobile, testbed-oriented living lab setting*, Mobile Networks and Applications **15**(3), 378 (2010)
7. A. Nieto, J. Lopez, *Security and QoS relationships in Mobile Platforms*, in *Computer Science and its Applications* (Springer, 2012), pp. 13–21
8. N. Clarke, S. Furnell, *Authenticating mobile phone users using keystroke analysis*, International Journal of Information Security **6**(1), 1 (2007). DOI 10.1007/s10207-006-0006-6
9. G. Anastasi, M. Conti, E. Gregori, A. Passarella, *Balancing energy saving and QoS in the mobile internet: an application-independent approach*, in *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on* (IEEE, 2003), pp. 10–pp
10. P. Bellasi, S. Bosisio, M. Carnevali, W. Fornaciari, D. Siorpaes, *Constrained Power Management: Application to a multimedia mobile platform*, in *Design, Automation Test in Europe Conference Exhibition (DATE), 2010* (2010), pp. 989 –992
11. Y.W. Kao, G.H. Luo, H.T. Lin, Y.K. Huang, S.M. Yuan, *Physical Access Control Based on QR Code*, in *Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2011 International Conference on* (2011), pp. 285 –288. DOI 10.1109/CyberC.2011.55
12. P. Kieseberg, M. Leithner, M. Mulazzani, L. Munroe, S. Schrittwieser, M. Sinha, E. Weippl, *QR code security*, in *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia* (ACM, New York, NY, USA, 2010), MoMM '10, pp. 430–435. DOI http://doi.acm.org/10.1145/1971519.1971593
13. W.B. Cheon, K. il Heo, W.G. Lim, W.H. Park, T.M. Chung, *The New Vulnerability of Service Set Identifier (SSID) Using QR Code in Android Phone*, in *In-*

formation Science and Applications (ICISA), 2011 International Conference on (2011), pp. 1 –6. DOI 10.1109/ICISA.2011.5772367
14. G.V. Damme, K. Wouters, *Practical Experiences with NFC Security on mobile Phones*, Katholieke Universiteit Leiden (2009)
15. G. Madlmayr, J. Langer, C. Kantner, J. Scharinger, *NFC Devices: Security and Privacy*, in *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on* (2008), pp. 642 –647. DOI 10.1109/ARES.2008.105
16. C. Mulliner, *Vulnerability Analysis and Attacks on NFC-Enabled Mobile Phones*, in *Availability, Reliability and Security, 2009. ARES '09. International Conference on* (2009), pp. 695 –700. DOI 10.1109/ARES.2009.46
17. R. Verdult, F. Kooman, *Practical attacks on NFC enabled cell phones*, in *Near Field Communication (NFC), 2011 3rd International Workshop on* (IEEE, 2011), pp. 77–82
18. M. Roland, J. Langer, J. Scharinger, *Security Vulnerabilities of the NDEF Signature Record Type*, in *Near Field Communication (NFC), 2011 3rd International Workshop on* (2011), pp. 65 –70. DOI 10.1109/NFC.2011.9
19. W. Glisson, T. Storer, G. Mayall, I. Moug, G. Grispos, *Electronic retention: what does your mobile phone reveal about you?*, International Journal of Information Security **10**, 337 (2011). 10.1007/s10207-011-0144-3
20. M. Uddin, S. Haseeb, M. Ahmed, A.S. Pathan, *Comprehensive QoS analysis of MIPL based mobile IPv6 using single vs. dual interfaces*, in *Electrical, Control and Computer Engineering (INECCE), 2011 International Conference on* (2011), pp. 388 –393. DOI 10.1109/INECCE.2011.5953912
21. S. Kiminki, V. Saari, V. Hirvisalo, J. Ryynanen, A. Parssinen, A. Immonen, T. Zetterman, *Design and performance trade-offs in parallelized RF SDR architecture*, in *Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM), 2011 Sixth International ICST Conference on* (IEEE, 2011), pp. 156–160