A. Nieto, and J. Lopez, "A Context-based Parametric Relationship Model (CPRM) to Measure the Security and QoS tradeoff in Configurable Environments", *IEEE International Conference on Communications (ICC'14)*, pp. 755-760, 2014.
http://doi.org/10.1109/ICC.2014.6883410
NICS Lab. Publications: https://www.nics.uma.es/publications

A Context-based Parametric Relationship Model (CPRM) to Measure the Security and QoS tradeoff in Configurable Environments

Ana Nieto, Javier Lopez
Computer Science Department
University of Malaga, Spain
Email:{nieto,jlm}@lcc.uma.es

***Abstract*—Heterogeneity of future networks requires the use of extensible models to understand the Security and QoS tradeoff. We believe that a good starting point is to analyze the Security and QoS tradeoff from a parametric point of view and, for this reason, in a previous paper, we defined the Parametric Relationship Model (PRM) to define relationships between Security and QoS parameters. In this paper, we extend that approach in order to change the behaviour of the model so that different contexts in the same system are considered; that is, to provide a Context-based Parametric Relationship Model (CPRM). The final aim is to provide useful tools for system administrators in order to help them deal with Security and QoS tradeoff issues in the configuration of the environment.**

***Index Terms*—Security; QoS; tradeoff; PRM; Context;**

I. Introduction and Background

There are models proposed in the literature that perform the Security and QoS tradeoff. However, generic-based models are unusual. Two examples of generic-based models related to our research topic are [1] and [2].

For example, [1] presents an approach for predicting the tradeoff between Security and QoS, using model checking to verify the equivalences between both specifications, in order to control illegal information flows in the system. Therefore, the tool-supported methodology proposed defines a communication model between applications. This makes the implementation of the solution more difficult. Another approach is followed in [2], where the AL-MODEL is used to provide a context-based model to balance QoS and Security. This model provides a utility function, taking into account the user preferences. But, although the model uses different types of contexts (computing, physical and user), and the utility function can express the preferences of the user, the impact of one parameter on the rest of the parameters cannot be set.

In our opinion, the Security and QoS tradeoff analysis should be based on parametric relationships between the different parameters that are part of the information system. Moreover, such an analysis has to be performed taking different contexts into consideration. The advantage of using parametric relationships is that it is possible to infer the dependability of one parameter on the rest of parameters.

An example of a rule-based parametrization technique was used in [9] to provide QoS-reconfigurable services in *Service Oriented Architecture* (SOA). This approach is specific to a type of system but it is interesting as an example of parametric-based reconfiguration. Moreover, there are a number of results related to Security and QoS tradeoffs focusing on specific environments that cannot be ignored [6][10] [7].

For example, [6] provides a set of frameworks that provide Security and QoS self-optimization in *Mobile Ad-Hoc Networks* (MANET). The multilayer QoS architecture and the parameters considered in [6] can be easily defined according to a *Parametric Relationship Model* (PRM), and then added to a PRM-based system. This provides the opportunity to expand this architecture, and use it with additional parameters that had not been previously considered in [6]. So, the Security and QoS tradeoff focusing on a specific environment can be used as the context from where to extract useful data to be later used for making decisions in configurable environments. The idea is provide the mechanisms for extracting parameter-based information so as to analyze this information in an independent-technology system in order to measure the impact that security mechanisms have on a QoS-based system.

In a previous paper [5], we proposed a solution for the implementation of the PRM. This one provides a language where different parameters can be represented, as well as their relationships. Thus, using that model, and given a relationship $A \rightarrow B$, it is possible to extract the influence on parameter B, the dependence on parameter A, and the impact on the system when a parameter increases or decreases its value.

This is very useful in order to determine the Security and QoS tradeoff in a system. However, the main problem with such a solution is that the context is not considered. Therefore, all the parameters, relationships and dependencies have the same relevance in the system, but this is unrealistic because all systems depend on a context. More specifically, and as we concluded in [4], the systems have general parameters and specific parameters that are, in the end, considered together. So, defining a *Contextual-based Parametric Relationship Model* (CPRM) is, to our understanding, the natural step towards evaluating the security and QoS tradeoff in a system.

For that reason, in this paper, we provide a sustainable analysis of a context-based module for PRM in order to adapt the behaviour of the system to work with a *General Context* (GC) and a *Particular Context* (PC). Moreover, the proposed extension allows the exchange of contexts between

Table I
PARAMETRIC RELATIONSHIP MODEL DEFINITIONS.

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

Acumulative Influence (ι)		Acumulative Dependence (δ)	
$\iota(a) = \lvert I_a \rvert = \lvert \{x \lvert x \rightarrow a \vee xRa, x \neq a, x \in P\} \rvert$	(10)	$\delta(a) = \lvert D_a \rvert = \lvert \{y \lvert a \rightarrow y \vee aRy, y \neq a, y \in P\} \rvert$	(11)
		$xRy \iff x \rightarrow y \vee \exists k \lvert k \in D_x \wedge k \in I_y$	(12)

Impact Increasing (Δ) and Decreasing (∇) a Parameter x

$$u(x,\omega) = \begin{cases} \Delta x & \text{if } \omega > 0; \\ \nabla x & \text{if } \omega < 0; \end{cases} \quad (13)$$

$$\Delta x \implies \forall y \lvert xRy, v(y) = v(y) + \Omega(R, \Delta x) \wedge u(y, \Omega(R, \Delta x)) \quad (14)$$

$$\nabla x \implies \forall y \lvert xRy, v(y) = v(y) + \Omega(R, \nabla x) \wedge u(y, \Omega(R, \nabla x)) \quad (15)$$

$\Omega(R, op(x))$, $R \in \{+, -, \neg +, \neg -, c, t, \neg c, i+, i-\}$, $op \in \{\Delta, \nabla\}$: (16)

	$+$	$-$	$\neg +$	$\neg -$	c	t	$\neg c$	$i+$	$i-$
Δx	$w_{x,+}$	$-w_{x,-}$	ntd	ntd	$w_{x,c}$	$w_{x,t}$	$-w_{x,\neg c}$	$w_{x,i+}$	$-w_{x,i-}$
∇x	ntd	ntd	$-w_{x,\neg +}$	$w_{x,\neg -}$	$-w_{x,c}$	$-w_{x,t}$	$w_{x,\neg c}$	$w_{x,i+}$	$-w_{x,i-}$

CPRMs. In our opinion, the context in a system is defined based on the parameters present in the system (defined at different layers and of distinct types), the relevance of each parameter to the system (what really matters in the system, administrative decisions) and the real impact of each parameter on the system (depends on the mechanisms and technologies used, and cannot be subjective).

One possible way of setting up the context in a system is to target the relevant components with weights in order to show their importance and impact. Based on the previous definition of context, it can be understood that we need, as minimum requirements, weights for each parameter (A and B), to measure their relevance, and for each relationship, to measure the impact that, for example, an increment of A has on B. But, as we will show later, additional weights need to be considered in order to correctly define a context.

The rest of the paper is structured as follows. In Section II, an overview of the PRM is provided in order to introduce the base system which supports the extensions provided here. Section III explains the CPRM architecture and the main changes over the previous model to enable the changes based on the behaviour. Finally, in Section IV, an analysis of the proposed CPRM approach is presented. The conclusions are summarized in Section V.

II. PARAMETRIC RELATIONSHIP MODEL

The Parametric Relationship Model (PRM) has been defined so as to provide a common language for defining and evaluating the Security and QoS tradeoff in generic environments. The model defines a set of parametric relationships in order to express the dependencies between different types of parameters and a set of rules to perform basic query operations over the parameters. More detailed information on the operations performed by the model and some examples of the application of the rules can be found in [4] and [5]. A brief description of the formulation related to the PRM can be seen in Table I.

The PRM provides a *Basic Formulation Set* (BFS) which defines the basic behaviour of the system when a parameter x is increased (Δx) or decreased (∇x). The *Complex Formulation Set* (CFS) is based on the BFS. The CFS is used for simplicity when the relationships between the parameters of the system are defined. Moreover, the model allows general information about the parameters defined in accordance with the model to be extracted. In particular, the *Acummulative Influence* on a parameter a ($\iota(a)$), shows the total number of parameters the modification of which affects a, while the *Acumulative Dependence* on a ($\delta(a)$) shows the total number of parameters, the value of which is modified if a changes (increases Δ or decreases ∇). Both ι and δ are independent from the type of relationship R (BFS or CFS)[1].

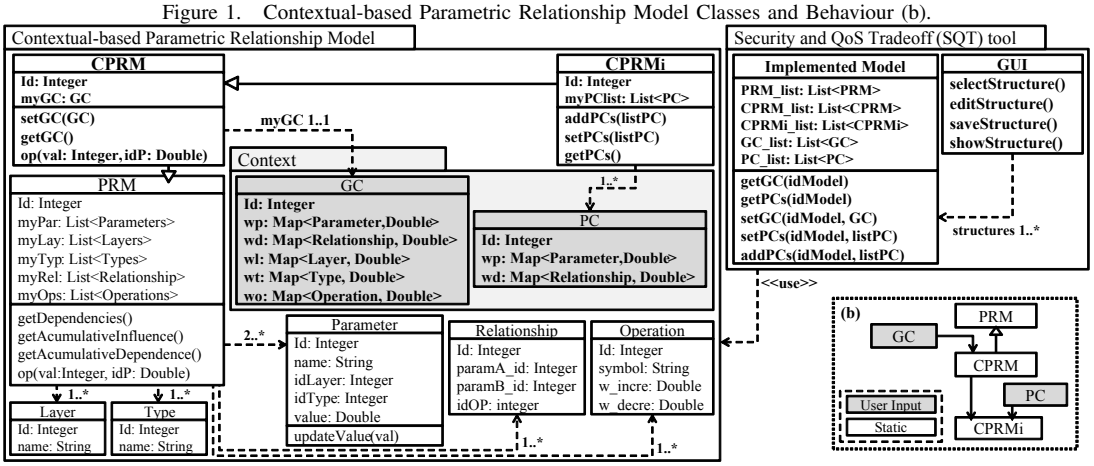
R is taken into account when the impact of increasing (Δ) or decreasing (∇) a parameter is calculated. In such cases, the value of the parameter in the consequent of the relationship varies depending on the relationship R. According to the definition of BFS and, therefore CFS, the value in the consequent is expressed through $\Omega(R, op(x))$ (Table I.(16)). For example, if the relationship between the parameters A and B is positive ($A \xrightarrow{+} B$), then when A increases, the parameter B also increases, given a value which depends on B and the relationship $+$ ($w_{B,+}$). However, when A decreases, given the relationship $+$, there is no additional information to be considered and, therefore, there is *nothing to do* (ntd)[2]

In this model, $w_{x,R}$ is equal to 1 for all the parameters and relationships. So, all the parameters are considered as equally relevant. Moreover, although $w_{x,R}$ are different from 1, there are additional weights that should be set up in order to properly define the behaviour of a dynamic environment. For example, considering that a parameter can be targeted with a type or can belong to a particular layer of abstraction [5], it would be useful to enable administrators of the system to configure the model, taking into account the relevance of those types or layers in the environment in a specific moment or context.

[1] R is also denoted as $d(x, y)$.

[2] Note that A and B can be set of parameters. Moreover, a requirement can be seen as a parameter. In that case, the requirement can be provided or not.

Figure 1. Contextual-based Parametric Relationship Model Classes and Behaviour (b).



III. Context-based Parametric Relationship Model (CPRM)

As mentioned, CPRM is an enhancement of the previous model so as to be able to interpret different types of contexts. This can be understood from various points of view. First, it is able to distinguish between *general contexts* (GC) and *particular contexts* (PC). Second, in order for the final CPRM-based system to be extensible and allow a grain-fine configuration, it has to take into account different types of weights: for each parameter (w_p), dependency $\rightarrow$ (w_d), type of parameter (w_t), layer (w_l), and operation (w_o).

It is understood that, while some of these weights can never change, others may vary according to a specific context. So, in the solution proposed, GCs define the general behaviour of the system, and PCs define the parameters used to support the requirements and other general parameters described in GC.

The PRM has to be updated in order to consider the GC and the PC. To allow this, and also to enable separation of the GC and PC from the PRM, we define the CPRM structure, which is a PRM with general weights, and also the instance of a CPRM ($CPRM_i$), which is the instantiation of a CPRM based on a PC. Figure 1 shows the components in a CPRM-based system, as well as the process followed in order to obtain a $CPRM_i$ (b). $CPRM_i$ represents the final behaviour of the system, in which all the mechanisms and technologies that are relevant are finally chosen by the administrator and taken into account when extracting relevant information of the model. The user/administrator sets the contexts using the GUI. The $CPRM_i$ can integrate various PCs, but only a GC.

Finally, dividing the overall context into general and specific ones, enables the context to be modified separately. So, the GC in a $CPRM_i$ can be changed, as well as the PCs. Subsequently, rules are applied to maintain the coherency in the model. In other words, the behaviour of the model can change based on the *Action Rules* (AR), that are used when a rule is not satisfied, hence making the model consistent again. AR are defined according to the rules shown in Table II. Note that A3 enables a parameter to collaborate with any other parameter defined as a consequent of the dependence of any of its parents. However, in the current implementation, A3 is applied if and only if there is no child of k related with x ($\nexists p|k \in P(p) \wedge d(x,p)$). By doing this, the user can force any instance of the parameters to be solely related to a set of instances of another parameter. In any case, R2 and the property of inheritance in R3 have to be maintained.

The modification of the equations defined for the PRM was carried out in order to consider the integration with the GC. The integration with the PC is defined for the CPRM and is based on a set of rules for performing the instatiation of the CPRM based on the PC. We show both processes in the following sections.

A. Modifications in the Model: Setting up a General Context

Equations (10-12) contained in Table I do not change, because those formulations are independent from the context.

$$\Delta x \implies \forall y|xRy, v(y) = v(y) + w_T \wedge u(y, w_T) \quad (17)$$
$$\nabla x \implies \forall y|xRy, v(y) = v(y) + w_T \wedge u(y, w_T) \quad (18)$$

However, Equations (14-15) change into (17-18), in order to add the *total weight* (w_T) based on the weight for the parameter in the antecedent (w_p), the type (w_t) and layer (w_l) of that parameter, and the weight for the operation w_o. Regarding w_o, in this definition it is independent from the weights in Ω ($w_{x,R}$). Ω shows the information given by the definition of the BFS and CFS (1-9), while w_o takes a subjective value.

$$w_T = (\Omega w_d)\frac{w_p + w_o + w_t + w_l}{max_p + max_o + max_t + max_l} \quad (19)$$
$$w_d(a,b) > 0 \ \forall a, b|aRb \quad (20)$$

Note that w_p, w_t, w_l and w_o can be subjective. However, w_d should be defined according to the true effect that the parameter in the antecedent (aka x) has on the parameter in the consequent (aka y) given the relationship R and the action performed a ($\Delta or \nabla$). Moreover, w_d should be propagated to the rest of the dependencies in the chain.

Equation (20) adds an additional condition to build the GC: w_d is at least equal to 1, because if there exists a relationship

Figure 2. Instantiation.

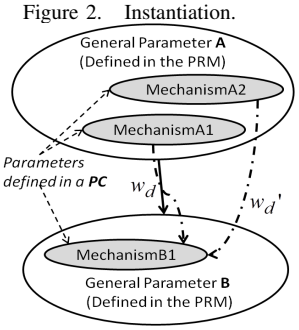


Table II
RULES AND ACTION RULES (AR).

Rule	Action Rule
R1 A parameter in the PC is related to at least one parameter in the PRM (parents).	A1 If not, the independent parameter is considered as one new parent and added to the PRM to make it consistent.
R2 Given P(x) and P(y) the list of parents of x and y, respectively $\|P(x) \cup P(y) \subset PRM$. If d(x,y), exists, then $\exists k \in P(x) \wedge \exists z \in P(y) \| d(k,z)$.	A2 Otherwise, said relationship between parents has to be added to the PRM in order to make it consistent.
R3 A parameter in the PC inherits the relationships of its parents, by default: if z belongs to P(x) and d(z,k), then d(x,k) is possible, with weight w(z,k) by default.	A3 The relationship d(x,k) is added with w(z,k) $\forall k$. If $\exists p \| k \in P(p)$ and therefore, according to R2, $d(x,p)$, w(x,p) don't change.
R4 A parameter x inherits the layer of its parents and the type of its parents. When $\exists k, z \in P(x) \| type(k) \neq type(z)$, then $type(x) = [type(k) type(z)]$.	A4 The decision model can fix the type of the layer of a parameter, but, even so, the final layer and type match with the layer and type of a parameter p in P(x).

between two parameters then there is an effect on the system to be measured. The current implementation of the model permits setting up any value for weights but, when w_d is equal to 0, then the w_T is also 0.

Using the aforementioned formulation it is feasible to perform the operations previously used in the PRM, but using a given context based on weights. However, it is necessary to provide new rules and action rules in order to keep the model coherent when certain parameters are introduced by an administrator during the execution of the CPRM-based tool for administration.

In order to provide the functionality needed to introduce a PC and match it to the CPRM, we provide definitions for a PC, rules to make it consistent with the current GC in the CPRM, and rules to decide how the different types of parameters cohexist and are taken into account.

B. Considerations for a Particular Context: Rules, Coherence and Instatiation

The action rules shown in Table II are taken into account when a PC is used to instantiate a CPRM. However, before setting up the rules, a new structure is needed in order to represent an instance of the CPRM. The $CPRM_i$ has to be defined taking into consideration a set of requirements:

- Independence from the original CPRM.
- Coherence between parameters in the model (Table II).
- Adaptation capability: acceptance of new PC to be added to the existing one.
- Capability to return to the original CPRM behaviour.

Although CPRM is an extension of PRM in order to consider context-based behaviour, $CPRM_i$ has to be considered as an *instantiation of a CPRM based on a PC*. The $CPRM_i$ is not a new version of PRM or CPRM, because its purpose is not to define a model or implement functions. Actually, its purpose is to change its behaviour based on different contexts. Thus, a $CPRM_i$ is always built based on a CPRM and a PC, but when it is created, the original data in the CPRM should be cloned in the $CPRM_i$ in order to make it independent.

The current definition of $CPRM_i$ has been built, based on the following steps:

1) The $CPRM_i$ adds the special types *Instance* and *Instantiated* to the model.
2) The type Instance will be the type in the model for the parameters included from the PC. Of course, during the inference process the given parameters take the original type of their parents according to a set of rules. With these tags in the model it is possible to properly identify which parameters belong to a given PC. As a result, it is possible to return to the original CPRM behaviour.
3) If a parameter y is Instantiated, that is, if $\exists x \in PC | y \in P(x)$, then in the $CPRM_i$ the parameter becomes a new layer. The new layers which represent instantiated parameters are separated from the rest of the layers defined in the model. When the PC is retrieved, the parameters which cease to be instantiated return to the original list of parameters in the model.
4) When the $CPRM_i$ receives a new PC, the new parameters are integrated in order to maintain the coherence in the model, based on the rules in Table II.

Then, when an instantiated parameter is represented as a layer, this adds the possibility of calculating the effect that the whole layer has on the performance of the system, thereby making it possible to evaluate the tradeoff between different mechanisms. The composition of parameters is shown in Figure 2, where the parameters A1, A2 and B1 are instances of A and B. The approximate weight for a general relationship $A \Rightarrow B$, w_d, is replaced by the specific weight, w'_d defined for $A2 \Rightarrow B1$. Moreover, $A1 \Rightarrow B1$ uses the general weight w_d because there is not a specific weight defined for it.

IV. ANALYSIS

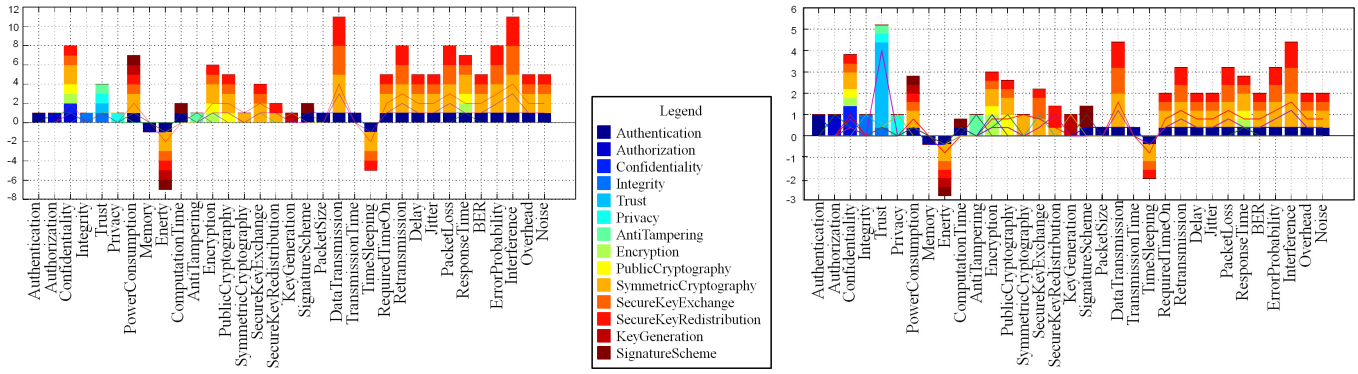
In order to show how a CPR-based system works, we provide an example based on wireless sensor networks (WSN). The initial parameters considered here, are taken from [4], [5]. These are used to build the GC.

The following subsections show the results when the relevance for the parameters, layers or types (given by w_p, w_l and w_t) changes in a particular scenario, and when the values w_d are provided according the results in [3].

A. Setting up the Relevance (w_p)

In a PRM, all the parameters have the same relevance ($w_p == 1, \forall p$). In order to indicate the relevance of a parameter in a CPRM, we target each parameter with a

Figure 3. Increase Security.



(a) $w_p == 1, \forall p \in PRM$

(c) $w_{Trust} == 4$

different weight w_p. This is necessary to set up the minimum context for the system: namely which of the parameters are most important to an administrator at a given time.

For example, Figure 3(a) shows the effect on the system when security parameters are decreased, and all the parameters are weighted with 1. In Figure 3(c) the process is repeated with the weight for Trust modified to 4.

Increasing or decreasing the values for w_t and w_l have similar consequences. These weights are used in order to make the representation of different contexts in the system possible (ej. increase the relevance of parameters of type *security*). Moreover, they can be considered as subjective values which can even represent particular needs or requirements in a network (e.g. increase the relevance of Authentication in the presence of guests in a network).

However, in order to perform the Security and QoS tradeoff we need to compare different alternatives. So, probably, the most interesting change in the CPRM-based system is when the administrator sets up a PC. In the PC, specific mechanisms are considered as instances of general parameters[3]. In our case, the main objective is to design the CPRM-based system in order to perform the Security and QoS tradeoff. Thus, the next step is to show how security parameters in the GC can be instantiated in order to evaluate the final impact that security mechanisms have on the system.

B. Setting up Weights in Dependencies (w_d)

In a PC, the instances of parameters can be targeted with particular weights according to the context. This is very useful when we want to indicate the impact that a particular mechanism (instance of a general parameter) has on any other parameter in the final context. In such cases, the context is set up in the dependencies using w_d. Unlike w_p, the value of w_d will be *propagated* throughout the dependency chain.

Moreover, the AR enable the adaptation of the model for the inclusion of direct dependencies between specific parameters and general parameters. For example, from [3], different types of sensors using different key exchange protocols may affect the energy in the environment differently. In this case, with the current parameters considered, it is possible to instantiate the general parameter *Secure Key Exchange* by the algorithms ECMQV, SOK and SC-ECMQV (new parameters), given PCs for sensors of type MICA or UWM. Then, following the values in Table 2 of [3] proportionally, the weights for the new dependencies in the PC (w_d) can be set up in accordance with Table III.

Table III
WEIGHTS w_d ACCORDING TO [3].

P.Context	Dependence			Weight
	Antecedent	Relationship	Consequent	w_d
MICA2	ECMQV	c	ComputationTime	4
	SOK	c	ComputationTime	5
	SC-ECM1V	c	ComputationTime	3
	ECMQV	$\neg c$	Energy	6
	SOK	$\neg c$	Energy	2
	SC-ECM1V	$\neg c$	Energy	3
UWM2000	ECMQV	c	ComputationTime	4
	SOK	c	ComputationTime	5
	SC-ECM1V	c	ComputationTime	3
	ECMQV	$\neg c$	Energy	21
	SOK	$\neg c$	Energy	39
	SC-ECM1V	$\neg c$	Energy	71

There are two key points to highlight here. First, in this particular example, the new parameters defined in the two new PCs are the same. The difference between them is the definition of the relationships for the weights. Second, as a consequence, it would be easy to think of using the same PRM to define the relationships and two GC for defining different weights in the dependencies. However, this is the wrong way to proceed. In fact, one of the advantages of our approach is that the GC can be set up as an static state, guaranteeing minimal modifications over a general context. Then, the GC should be chosen to perform low modifications over it (similar to an axioma), while the PC is defined to make continuous changes over the environment.

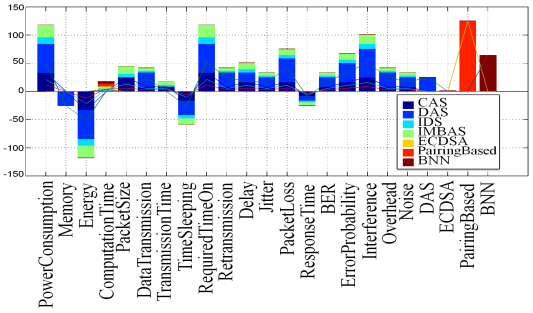
Note that, both contexts define direct dependencies with the

[3]For example, the instantiation can be done by providing a property.

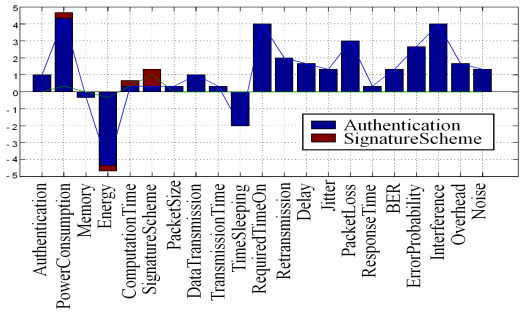
Table IV
WEIGHTS w_d ACCORDING TO [8].

General Parameter	Dependence			Weight
	Antecedent	R	Consequent	w_d
Authentication	CAS	+	ECDSA	1
	DAS	+	ECDSA	1
	IDS	+	PairingBased	1
	IMBAS	+	BNN	1
	CAS	$\neg c$	Memory	0
	DAS	$\neg c$	Memory	5
	IDS	$\neg c$	Memory	0
	IMBAS	$\neg c$	Memory	0
	CAS	c	PacketSize	5
	DAS	c	PacketSize	1
	IDS	c	PacketSize	3
	IMBAS	c	PacketSize	4
Signature Scheme	ECDSA	$\neg c$	Energy	1
	PairingBased	$\neg c$	Energy	5
	BNN	$\neg c$	Energy	4
	ECDSA	c	Computation Time	1
	PairingBased	c	ComputationTime	5
	BNN	c	ComputationTime	4

Figure 4. Impact on the Environment given the context in [8].



(a) Particular View: Instance of parameters.



(b) General view: Instantiated Parameters.

final nodes in the GC[4], therefore if only the parameter *Secure Key Exchange* is modified, the final information is not much more illustrative than in [3]. The real advantage of CPRM can be seen when it instances several types of parameters.

For instance, another example of a particular context is given in [8]. The relationships for this context are defined in Table IV. In this case, the parameters to be instantiated are *Authentication* and *Signature Scheme*. Figure 4 shows the impact that the PC has on the CPRM-based system. In this example, indirect relationships affect the other parameters related to performance that are in the CPRM but were not considered in [8].

[4]Computation time and energy do not act as antecedents in any dependence in the model.

V. CONCLUSIONS

In this paper, we have provided a Context-based Parametric Relationship Model (CPRM), which extends the PRM definition given in [5] in order to make it useful for modeling context-based scenarios. This approach divides the context into *General Context* and *Particular Context* in order to provide a puzzle-based solution, where the administrator of the system can exchange the contexts in order to make decisions on the ideal configuration to perform the Security and QoS tradeoff. The CPRM-based system has been implemented using MATLAB, and examples of the approach have been applied. CPRM is independent from the applications because it considers the properties/configuration taken by the applications or systems to perform the parametric relationship analysis.

ACKNOWLEDGMENT

This work has been partially supported by the Spanish Ministry of Economy and Competiveness through the projects SPRINT (TIN2009-09237) and ARES (CSD2007-00004), being the first one 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.

REFERENCES

[1] Alessandro Aldini and Marco Bernardo. A formal approach to the integrated analysis of security and qos. *Reliability Engineering & System Safety*, 92(11):1503–1520, 2007.

[2] Mourad Alia, Marc Lacoste, Ruan He, and Frank Eliassen. Putting together qos and security in autonomic pervasive systems. In *Proceedings of the 6th ACM workshop on QoS and security for wireless and mobile networks*, pages 19–28. ACM, 2010.

[3] David Galindo, Rodrigo Roman, and Javier Lopez. On the energy cost of authenticated key agreement in wireless sensor networks. *Wireless Communications and Mobile Computing*, 12(1):133–143, 2012.

[4] Ana Nieto and Javier Lopez. Analysis and taxonomy of security/qos tradeoff solutions for the future internet. *In Security and Communication Networks, Security in a Completely Interconnected World*, In Press.

[5] Ana Nieto and Javier Lopez. A model for the analysis of qos and security tradeoff in mobile platforms. *In Mobile Networks and Applications, Developments in Security and Privacy-preserving mechanisms for Future Mobile Communication Networks*, In Press.

[6] ZhengMing Shen and Johnson P Thomas. Security and qos self-optimization in mobile ad hoc networks. *Mobile Computing, IEEE Transactions on*, 7(9):1138–1151, 2008.

[7] Akash Singh. Optimal qos attributes in security key management and interoperability between heterogeneous federation architectures. *International Journal of Computational Engineering Research*, 2012.

[8] Rehana Yasmin, Eike Ritter, and Guilin Wang. An authentication framework for wireless sensor networks using identity-based signatures. In *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, pages 882–889. IEEE, 2010.

[9] I-Ling Yen, Hui Ma, Farokh B Bastani, and Hong Mei. Qos-reconfigurable web services and compositions for high-assurance systems. *Computer*, 41(8):48–55, 2008.

[10] Wente Zeng and Mo-Yuen Chow. A trade-off model for performance and security in secured networked control systems. In *Industrial Electronics (ISIE), 2011 IEEE International Symposium on*, pages 1997–2002. IEEE, 2011.