A. Nieto, N. Nomikos, J. Lopez, and C. Skianis, "Dynamic Knowledge-based Analysis in non-Secure 5G Green Environments using Contextual Data", *IEEE Systems Journal*, vol. 11, pp. 2479-2489, 2017.
http://doi.org/10.1109/JSYST.2015.2477782
NICS Lab. Publications: https://www.nics.uma.es/publications

Dynamic Knowledge-based Analysis in non-Secure 5G Green Environments using Contextual Data

Ana Nieto, Nikolaos Nomikos, Javier Lopez and Charalambos Skianis

***Abstract*—The growing number of parameters in heterogeneous networks, as is the case of the *fifth generation* (5G) Green networks, greatly complicates the analysis of the *Security and Quality of Service Tradeoff* (SQT). However, studying these types of relationships is crucial in Future Internet scenarios to prevent potential points of failure and to enhance the use of limited resources, increasing the user's experience. Therefore, it is fundamental to provide tools and models for training, so that the users understand these dependencies and solve them prior to deploying new solutions. In this paper, a Recommendation System for SQT (SQT-RS) is deployed in 5G Green systems, considering the particular case of relay networks and the impact of eavesdropping and jamming contexts on the models generated by the user, aided by SQT-RS. With this goal in mind, we provide a component for the user to automatically select specific contexts based on 5G Green capabilities.**

***Index Terms*—Context, Knowledge based systems, Green design, Cellular networks, Communication system security.**

I. Introduction

Recently, research into wireless networks has focused on the development of 5G enabling technologies, building on the achievements of the previous generations, aiming to enhance the *Quality of Service* (QoS) offered to the users. However, the economic and environmental sustainability of 5G networks has to be promoted through the Green Communications paradigm, targeting the reduction of the operational cost of the network, as well as its carbon footprint. So, technologies that offer energy-efficient QoS will play a major role [1]. To this end, cooperative relaying improves the wireless channel's characteristics through mutlti-hop transmissions and multi-path fading mitigation via increased diversity [2]. In cases where buffer-aided relays are available, interesting tradeoffs arise between increased diversity and controlled delay [3]. These technologies are exposed to a wide number of attacks as analysed in [4], some of which can be mitigated when relay selection is implemented considering physical-layer security techniques [5]. For example, relay selection can result in avoiding the eavesdropper if *Channel State Information* (CSI) is available. Moreover, cooperative jamming can be employed to produce artificial noise and confuse the eavesdropper, as long as the trusted nodes' QoS is guaranteed.

In a 5G Green relay environment, the nodes can cooperate to send information to the destination, generating large amounts of data, from which information about the user's preferences, network performance, and QoS can be inferred [6]. This information can be useful to identify the effect that different technologies and configurations have on security and QoS. These dependencies at different layers at a given moment can be understood as the context of a system [7]. As 5G Green relay networks can involve from low-complexity personal devices to more powerful devices, assessing the security and QoS tradeoff is highly complex; it depends on the mechanisms to be deployed in a heterogeneous, dynamic and unpredictable environment. However, the final configuration of the environment cannot be independent from the analysis of the security and QoS tradeoff [8]

In this paper, a *Security and QoS Tradeoff Recommendation System* (SQT-RS) [9] is used in 5G Green parametric-based systems to provide recommendations based on different goals, and contexts are generated dynamically, based on the user's input. SQT-RS has been implemented to provide recommendations in *Context-based Parametric Relationship Model* (CPRM) compliant scenarios with large numbers of parameters [7]. Specifically, in this paper we provide:

- A description of how SQT-RS considers the identification of conflicts in the inference process.
- The definition of Green 5G-based CPRM systems. The relevant parameters for the analysis and the motivation for this selection is justified. We include parameters at different layers in the analysis.
- Dynamic generation of contextual models based on the inputs received from the user, considering a pre-defined fuzzy environment, and threat contexts.
- Evaluation of SQT-RS considering the particular use case of 5G Green relay. In this step, recommendations are generated according the user's preferences and goals.

The rest of the paper is structured as follows. Section II provides the related work to our approach. Section III describes the improvements in SQT-RS. Section IV provides the 5G Green parameters considered and the specific contexts and goals. Finally, the solution is implemented, and some results are shown in Section V. Conclusions and future lines

Manuscript received...

A. Nieto and J. Lopez are with the Department of Computer Science, University of Malaga, Campus de Teatinos 29071, Malaga, Spain (E-mails: {nieto, jlm}@lcc.uma.es).

N. Nomikos and C. Skianis are with the Department of Information and Communication Systems Engineering, University of the Aegean, Karlovassi 83200, Samos, Greece (E-mails: {nnomikos, cskianis}@aegean.gr).

This work has been supported by Junta de Andalucia through the project FISICCO (TIC-07223), and by the Spanish Ministry of Economy and Competitiveness through the project PERSIST (TIN2013-41739-R). The first author has been funded by the Spanish FPI Research Programme.

of research are discussed in Section VI.

II. Related Work

Although 5G relay networks bring with them several benefits they also pose challenges to be Green, as analysed in [10], [4], [11], [12]. For example, in [11], diverse methodologies for relay selection in 5G networks are described, and analysed from the point of view of performance and cost. Moreover, in [1] four challenges are identified that need to be addressed in 5G Green environments: (i) the increasing volume of data, (ii) the growing number of devices, (iii) the diversity of applications and (iv) the need for energy-aware solutions. In [6] the sources from where the data in 5G environments is generated are classified at different layers, from where it is possible to obtain the parameters to be analysed. For example, the user's information handled by the cells can help to identify the user mobility behaviour. In turn, it is possible to configure applications to improve the user's experience, as in [13], where an approach for balancing the data rate based on the user's context (e.g. location, time of the day) is provided, introducing tradeoffs related with power consumption. In addition, QoS delay constraints in 5G mobile networks are analysed in [14], and in [15] the challenges for handling high-volumes of data efficiently, considering energy restrictions and QoS support for real-time applications are discussed. The latest trends focus on defining *Software Defined Networks* (SDN) based architectures for 5G networks [16]. In this context diverse technologies and methodologies have been proposed and analysed [17], increasing the need for high-level composition of services, where the security and QoS tradeoff must be considered. Unfortunatelly, the different approaches for analysing the security and QoS tradeoff are focused on specific problems, or provide solutions at specific layers where the parameters in 5G Green relay networks are not addressed. Combining all these pieces together provide a large number of parameters, and this requires new solutions that enable the user to describe the context, target those parameters that really matter given the context, and understand the system behaviour before deploying the security and QoS mechanisms.

Therefore, 5G Green approaches handle a wide range of parameters at different layers. So, the security and QoS tradeoff must be analysed considering: (i) how to combine information from independent sources, and (ii) how to work with partial information - integrating new information when it is known. In this respect, CPRM, defined in [7], can help in analysing the security and QoS tradeoff considering (i-ii) in 5G Green environments.

III. SQT Recommendation System

In this section we focus on the improvements that have been made in SQT-RS. SQT-RS takes advantage of the properties of CPRM to enhance the selection of data and provide the recommendation sets, while being aware of the dynamic content. For this purpose, SQT-RS defines: (i) structures for goals and requirements, (ii) the concept of recommendation, and (iii) the dynamic generation of facts used as inputs for the recommendation system. Besides, SQT-RS is based on a set of rules to work in CLIPS [18]. The steps to build the facts and rules, from the selection of requirements and goals, is shown on the right-hand side of Figure 1. Table I provides the formulation that describes the behaviour of CPRM-based systems which has to be considered for implementing the recommendations.

Table I
Recursive operations in a CPRM-based system.

Accumulative Influence (ι) and Accumulative Dependence (δ)	
$\iota(a) = \lvert I_a \rvert, I_a = \{x \mid x \rightarrow a \vee xRa, x \neq a, x \in P\}$	(1)
$\delta(a) = \lvert D_a \rvert, D_a = \{y \mid a \rightarrow y \vee aRy, y \neq a, y \in P\}$	(2)
$xRy \iff x \rightarrow y \vee \exists k \mid k \in D_x \wedge k \in I_y$	(3)
Impact Increasing (Δ) and Decreasing (∇) a Parameter x	
$\Delta x \implies \forall y \mid xRy, v(y) = v(y) + w_T \wedge u(y, w_T)$	(4)
$\nabla x \implies \forall y \mid xRy, v(y) = v(y) + w_T \wedge u(y, w_T)$	(5)
$u(x,\omega) = \begin{cases} \Delta x & \text{if } \omega > 0; \\ \nabla x & \text{if } \omega < 0; \end{cases}$	(6)
${A_{D_{op}}}^{p} = \bigcup Dep(k)_{op'} \mid k \in D_p, op, op' \in \{\Delta, \nabla\}$	(7)

A. Inputs to SQT-RS

As Figure 1 shows, SQT-RS is used when a CPRM is provided. CPRM models are built dynamically, from general information (GC) to specific information given the context (PC). In the GC, general parameters are defined as general characteristics or properties to be satisfied, and in the PCs, specific parameters are provided to implement the parameters defined into the GC. This process is defined in [7] as *instantiation*, and the schemes that provide this information are denoted as $CPRM_i$. The parameters in the PC that define the specific behaviour to the parameters in the GC are denoted as *instances*, while the corresponding parameter in the GC are denoted as *instantiated*. We consider that either *instantiated* or *instance* parameters are contextual, while the rest of the parameters are considered as non-contextual parameters, as long as they are not modified due to the inclusion of a PC. The parameters in the model can be increased (Δ) or decreased (∇), thus affecting the other parameters. Until now, the CPRM schemes, GC, and PCs have been manually built, and the effect of the operations Δ and ∇ is analysed using graphs. The schemes are scripts written in Matlab, following the architecture of CPRMs, that describe the parameters, relationships, operations, types, layers, etc.

In this paper we add the *SQT 5G Green module* (SQT-5G) with two objectives: (i) to help for training users, and (ii) to allow the creation of CPRM schemes (.m files) to be used in SQT, based on a set of properties chosen by the user. These files are handled by SQT, and, therefore, the user can store and modify the files, extracting the PCs or integrating new ones. To do this, the *graphical user interface* (GUI) for SQT has been improved with the SQT-5G module. The parameters and their value in 5G Green are set up using the 5G selector module, which includes the use of fuzzy logic (Section IV).

The steps to build a CPRM or $CPRM_i$ (inputs to our system) using the 5G selector module are shown in Figure 1 (b). The user can select values for the parameters provided by the tool (1). Then, these parameters are integrated in

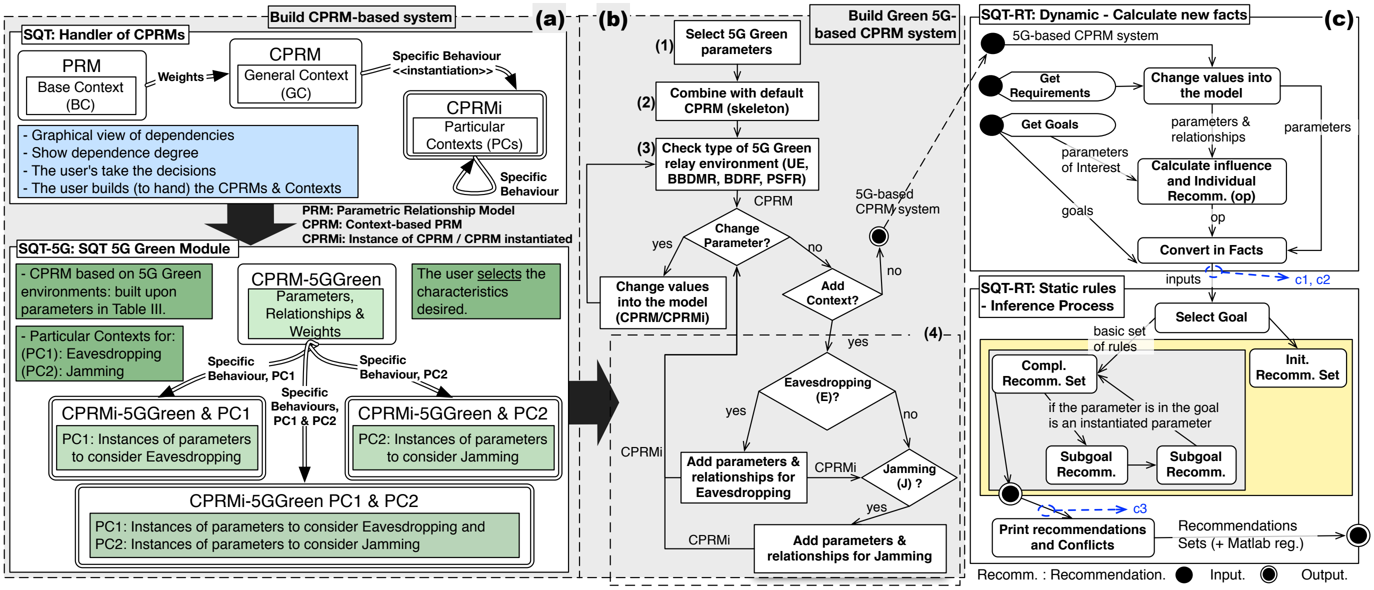

Build CPRM-based system
(a)
SQT: Handler of CPRMs
PRM
Base Context (BC)
Weights
CPRM
General Context (GC)
Specific Behaviour <<instantiation>>
CPRMi
Particular Contexts (PCs)
Specific Behaviour
- Graphical view of dependencies
- Show dependence degree
- The user's take the decisions
- The user builds (to hand) the CPRMs & Contexts
PRM: Parametric Relationship Model
CPRM: Context-based PRM
CPRMi: Instance of CPRM / CPRM instantiated
SQT-5G: SQT 5G Green Module
- CPRM based on 5G Green environments: built upon parameters in Table III.
- Particular Contexts for: (PC1): Eavesdropping (PC2): Jamming
CPRM-5GGreen
Parameters, Relationships & Weights
The user selects the characteristics desired.
Specific Behaviour, PC1
Specific Behaviour, PC2
Specific Behaviours, PC1 & PC2
CPRMi-5GGreen & PC1
PC1: Instances of parameters to consider Eavesdropping
CPRMi-5GGreen & PC2
PC2: Instances of parameters to consider Jamming
CPRMi-5GGreen PC1 & PC2
PC1: Instances of parameters to consider Eavesdropping and PC2: Instances of parameters to consider Jamming
(b)
Build Green 5G-based CPRM system
(1) Select 5G Green parameters
(2) Combine with default CPRM (skeleton)
(3) Check type of 5G Green relay environment (UE, BBDMR, BDFR, PSFR)
CPRM
Change Parameter?
yes
no
Change values into the model (CPRM/CPRMi)
Add Context?
no
5G-based CPRM system
yes
(4)
Eavesdropping (E)?
yes
no
CPRMi
Add parameters & relationships for Eavesdropping
CPRMi
Jamming (J) ?
yes
CPRMi
Add parameters & relationships for Jamming
SQT-RT: Dynamic - Calculate new facts
(c)
5G-based CPRM system
Get Requirements
Change values into the model
Get Goals
parameters & relationships
parameters
parameters of Interest
Calculate influence and Individual Recomm. (op)
goals
op
Convert in Facts
inputs
c1, c2
SQT-RT: Static rules - Inference Process
Select Goal
basic set of rules
Compl. Recomm. Set
Init. Recomm. Set
if the parameter is in the goal is an instantiated parameter
Subgoal Recomm.
Subgoal Recomm.
c3
Print recommendations and Conflicts
Recommendations Sets (+ Matlab reg.)
Recomm. : Recommendation.
Input.
Output.

Figure 1. Basic CPRM-5G Green scripts (a), 5G selector (b) and recommendation chain (c).

one skeleton with a default relationship set defined for the parameters (2). The 5G selector checks the type of 5G Green relay environment using fuzzy logic (3) (Section IV-A). At this point of the algorithm, the user can request to change the value of some of the parameters in the script. In such case, the type of 5G Green relay environment must be checked again. In other case, the system is prepared for integrating the specific behaviour provided by the two contexts for eavesdropping (E) and jamming (J) (4). As we can see in Figure 1, it is possible to integrate both contexts, only one of them or none.

The result of this process becomes one of the inputs for SQT-RS, together with the requirements and goals selected by the user. These are provided to get recommendations (Figure 1, c) as is detailed in the following sections.

B. Goals and Requirements

Goals and requirements are highly dependent on the user. SQT-RS provides a GUI for the selection of goals and requirements (Figure 4), and, internally handles these values using two structures: GOA and REQ (Expr. 8-11). The information in these structures is used to provide general descriptions, regarding the number of elements (#G, #Rec) and, then, the complete information of the user's goals and requirements.

$$GOA = \{\{\#G, CPRM_{id}, \#Rec\}; g_1; ...; g_{\#G}\}; \tag{8}$$
$$g_k = \{id, P_{id}, objective, S_{id}, C_{id}\}; \tag{9}$$
$$REQ = \{\{\#Req, CPRM_{id}\}; req_1; ...; req_{\#Req}\}; \tag{10}$$
$$req_k = \{id, Parameter_{id}, val\}; \tag{11}$$

The set of parameters shown in the GUI depends on the $CPRM_{id}$ selected in SQT, so any goal g_K is defined for a specific $CPRM_i$ at a given time, and is classified based on its identifier (id), an objective parameter given by its identifier (P_{id}), the objective or criterion to be applied, and a list of recommendations to satisfy the goal (S_{id}), which is initially set to null. Moreover, the list of conflicts identified for S_{id} is included in C_{id}. Both, S_{id} and C_{id} are uploaded into SQT-RS after the execution of the inference process in CLIPS.

Next, the requirements selected by the user are forced in the $CPRM_{id}$ target, modifying the values of the parameters. For this reason, the requirements do not store information about the recommendations. Instead, the requirements req_k are described using an identifier (id), the *id* of the parameter and the value taken by the parameter (val).

Two objectives are considered: maximisation (max) or minimisation (min) of the values of a parameter. For example, based on the classification of parameters in CPRM, parameters of type *consequence* or *performance* are good candidates to be considered as part of a goal. In a 5G Green environment, some parameters that may be chosen are *outage probability*, *signal strength*, *energy*, *secrecy capability*, *secrecy rate* and *complexity* between others. However, SQT-RS allows the selection of any parameter in the model as a goal.

C. Recommendation

A recommendation is described by the set of parameters and the operations to be performed in order to satisfy the goals requested by the user in the previous step. The formulation for recommendations in SQT-RS is provided in Table II: for one goal and one recommendation set as output (Expr. 12–13, 16–17, and 19), for several outputs or different recommendation sets (Expr. 14, 18, 20-21), and for multiple goals (Expr. 15). In this paper, we include the expressions 14-15 and 20-21. Sets of recommendations are provided when multiple goals cannot be satisfied simultaneously, or different combinations with different weights can be applied. The recommendations in a recommendation set S are ordered depending on the final impact on P, such that Expr. (20) is satisfied.

Note that Expr. (20) shows a property based on Expr. (16)-(17). So, when the recommendation is built, the final set of recommendations is composed by parameters that belong to the influence set of P (I_P) by definition (Expr. 1). For

Table II
FORMULATION FOR RECOMMENDATIONS.

Generic Definitions		
Goal:$g \in \{max, min\}, g :: CPRM \rightarrow [0, 1]$		(12)
Recommendation:$R = \{id1_{op_1}, ...idN_{op_N}\}$		(13)
Recommendations Set:$S_g(P) = \{R_1, ..., R_k\}$		(14)
Multiple objectives:$RS = \{S_{g1}(P_{id1}), ...S_{gq}(Pidq)\}$		(15)
Goal, $g(P)$	Recommendation	
$max(P)$	$R \vert id(x_j) = idj, x_j \in I_P, op_j(x_j) \rightarrow \Delta P$	(16)
$min(P)$	$R \vert id(x_j) = idj, x_j \in I_P, op_j(x_j) \rightarrow \nabla P$	(17)
$\Theta(R) = sum_{j=1}^{N} op_{jP}(x_j) \vert idj_{op_j} \in R, op_j \in \{\Delta, \nabla, \Box\}$		(18)
$\Box x \Rightarrow$ goal achieved by applying either Δx or ∇x		(19)
Prop. $R_i \in S_g(P), idj_{op_j} \in R_i, op_j(x_j) \rightarrow g(P)$		(20)
Prop. $S_g(P) = \{R_1, R_2\} \Leftrightarrow \Theta(R_1) > \Theta(R_2)$		(21)

multiple goals, it is probable that a single recommendation set S is unable to satisfy all the objectives and so, multiple recommendation sets can be provided, where the final goal for each set is to satisfy a subset of the overall set of goals. These types of multi-objective problems are too complex to solve by simple observation, and, depending on the number of parameters, can take a very long time to analysed.

According to the definition of a CPRM-based system, the *instances* provide richer information than their parents. Therefore, SQT-RS considers this and the parameters of type *instantiated* are not shown, instead, their instances are processed. Furthermore, SQT-RS only processes the information of those parameters that are related to one or more objectives.

D. Facts and Rules

The following sections detail the conversion of the information from the CPRM/$CPRM_i$ into facts, and the result of the operation on the CPRM parameters inside rules. Figure 1 shows the complete sequence used to build the facts and rules that are adopted by the expert system from a CPRM. .

1) CPRM-based facts: The list of facts generated by SQT-RS represents the current state of the model. This is built considering those parameters and relevant information extracted from the model which is related to the goals and preferences selected by the user. The process followed to build the list of facts is as follows:

i. The user selects the requirements for the parameters, and the goals (REQ and GOA are generated).
ii. REQ is set up in the model: the parameters required change their values to those selected by the user.
iii. The list of goals is processed to identify relevant parameters for the individual recommendations ($RSet$).
iv. The individual recommendations (*op*) are calculated based on Expr. (16)-(17).
v. The list of facts is generated.

Step (v) is performed by SQT-RS using templates in CLIPS and the definition of the relevant parameters, goals and individual recommendations based on the information in the model. The requirements, although not considered as facts, do influence the final recommendation by changing the value of the parameters in the CPRM. Note that, unlike the requirements, the goals selected by the user, are converted to facts without changing the model.

As a consequence, SQT-RS processes three types of input-facts, that are considered dynamic because they are generated when the user's preferences/inputs change the behaviour of a model: goals, individual recommendations (*op*, Expr. 16-17) and parameters. Additionally, SQT-RS generates *subgoals* when the parameter in a goal is instantiated, and *conflicts*.

Furthermore, *op*s reflect the operation to be carried out on a parameter in order to satisfy the user's goal, and are based on the results for increasing or decreasing those parameters which provide the best results to satisfy the goals.

a) Facts for identifying Conflicts: To provide a fine-grained identification of conflicts, it is necessary to identify those parameters in the chain of an individual recommendation, as well as the coincidences between the *internal operations* to achieve the goals.

We define the internal operations as facts ($internal - op$) to identify those intermediary parameters i, that influence the target/goal parameter g because their relationship with a parameter a is provided in an individual recommendation. In other words, $a \rightarrow ... \rightarrow i \rightarrow ... \rightarrow g$. Therefore, the intermediary parameters can be identified using the accumulative matrix of dependencies ${A_{D_{op}}}^a$ between the parameters in the selected CPRM (Expr. 7).

The drawback when including the facts $internal - op$ is that the number of facts increases considerably, because internal operations are defined per each parameter in the branch of the parametric trees. Therefore, the memory and processing time requirements of SQT-RS also increase. However, the benefit is that it avoids adverse effects that are produced because the application of individual recommendations affect the same parameters in the chain in opposite ways. In cases where both actions, Δ or ∇ a parameter, produce the opposite effect in the goal, the fact *avoid* is included to indicate that the recommendation that has been applied is the least damaging to achieve the objective, but the modification of the parameter should be avoided because it is opposite to the goal.

So, the CPRM-based rules defined in SQT-RS, by using the previous input-facts, will provide recommendations based on the result of applying operations on the parameters defined in the model (Table I) and the values to be enhanced as required by the user. Once the user receives feedback from the tool, new values can be introduced and then, the model generates new facts and the inference process starts again.

2) CPRM-based rules: The CPRM-based rules are static and never change. They are meant to satisfy the requirements for defining SQT-RS [9]. So, the inference process is divided into four steps:

1. Selection of a goal. Repeated for as long as there are goals to be processed.
2. Calculation of the set of recommendations, given the goal, that has to take into account whether the parameter is contextual or not.
3. Calculation of conflicts: before goal selection, or after the calculation of the recommendations, depending on the types of the considered conflicts.

Table III
SQT-RS PROPERTIES

Prop.	Antecedent	Conclusion ($\Rightarrow$)
1	$\exists op_j(x_j), x_j \in I_P, type(x_j) == T_P$	$\exists op_i(x_i), \forall x_i \| x_j \in P(x_i)$
2	$\exists g(x_j), type(x_j) == T_P$	$R_{g(x_j)} = R_{g(x_i)} \| x_j \in P(x_i)$
3	$\exists g(x_j) \Rightarrow x_j \in RSet$	$x_i \in RSet \Leftrightarrow x_j \in P(x_i)$
- Generic Assumptions in a CPRM -		
$\forall x_i x_j \in CPRM, x_j \in P(x_i) \Rightarrow (type(x_j) == T_P \land type(x_i) == T_C), T_P == instantiated, T_C == instance$		
$\forall x_j, \exists g(x_j) \Rightarrow x_j \in RSet$		

4. Print results. All the results are printed at the end of the inference process.

While 1 and 4 are basic steps, and step 3 depends on the concept of the determined conflict, the largest processing time appears in step 2, where rules are applied based on the type of parameter to be considered. The simplest rules in this phase are those which consider non-contextual parameters. The properties that describe the behaviour of SQT-RS regarding the contextual parameters are thoroughly detailed in [9], and summarised in Table III. These properties affect the individual recommendations (op), recommendations (R), and the parameters that are included in the set of interest ($RSet$).

a) Conflicts considered in the Rules: SQT-RS considers three cases of conflict:

- c1. When the modification of a parameter x, either increasing or decreasing, that is $\Box x$, precludes the goal.
- c2. When there is an intermediary parameter i that requires increasing and also decreasing to achieve the goal (opposing operations).
- c3. When different goals require opposite operations to satisfy their respective recommendations.

These conflicts are considered together, and, therefore, it is possible to print them at the same time as the recommendations are printed. The recognition of the conflicts based on the analysis of the attributes in simple facts (c1-c2) is available at the beginning of the recommendation process, while others being more complex, as they are based on the analysis of the final set of recommendations or multiple goals (c3), have to be analysed at the end of the decision process. For this reason, the identification of conflicts is performed before the selection of the next goal to be processed when c1 and c2 are considered, and at the end of the decision process, just after the recommendations for all the goals are ready, when c3 has to be considered (multiple goals).

Figure 2 shows an example of conflict because of c1 and c2. The conflict c2 occurs when the $A \rightarrow D$ and $A \rightarrow B$. The complete relationship c implies that when $\Delta A \Rightarrow \Delta B$ and when $\nabla A \Rightarrow \nabla B$ [7]. Therefore, to *max* B, the possible modifications in A have to be considered. However, when A increases, D also increases, and D has a negative relationship with B (-), which means that $\Delta D \Rightarrow \nabla B$. So, from the point of view of considering the modifications in A, D is an intermediary parameter that introduces a conflict when *max* B.

Another example is provided by the relationship defined by the instance of D, D1. This instance redefines the behaviour of D to modify the relationship with D to an independent negative

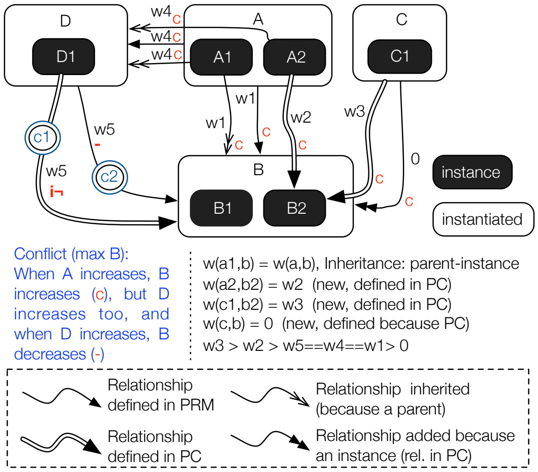
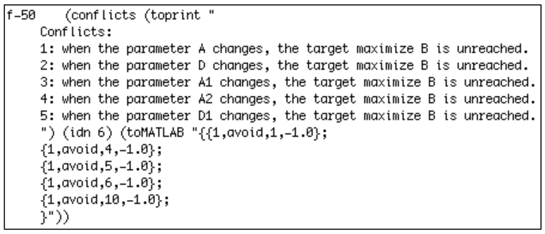

D
D1
A
A1
A2
C
C1
w4 c
w4 c
w4 c
w1
w1 c
c
w2 c
w3
c
0
c
c1
w5
i¬
w5
-
c2
B
B1
B2
instance
instantiated
Conflict (max B):
When A increases, B increases (c), but D increases too, and when D increases, B decreases (-)
w(a1,b) = w(a,b), Inheritance: parent-instance
w(a2,b2) = w2 (new, defined in PC)
w(c1,b2) = w3 (new, defined in PC)
w(c,b) = 0 (new, defined because PC)
w3 > w2 > w5==w4==w1> 0
Relationship defined in PRM
Relationship inherited (because a parent)
Relationship defined in PC
Relationship added because an instance (rel. in PC)

Figure 2. Example of inheritance relationships.



```
f-50    (conflicts (toprint "
     Conflicts:
     1: when the parameter A changes, the target maximize B is unreached.
     2: when the parameter D changes, the target maximize B is unreached.
     3: when the parameter A1 changes, the target maximize B is unreached.
     4: when the parameter A2 changes, the target maximize B is unreached.
     5: when the parameter D1 changes, the target maximize B is unreached.
     ") (idn 6) (toMATLAB "{{1,avoid,1,-1.0};
     {1,avoid,4,-1.0};
     {1,avoid,5,-1.0};
     {1,avoid,6,-1.0};
     {1,avoid,10,-1.0};
     }"))
```

Figure 3. Example: Internal fact in CLIPS generated for conflicts.

($i\neg$), that means that regardless of the modifications in D1, B always decreases when D1 is modified. So, this is a conflict of type c1 which affects the maximisation of B. As this type of conflict is visible when the individual recommendations are calculated, these types of conflicts are considered as facts of type *avoid*. Moreover, a recommendation is included to suggest the modification that affects the objective in the end.

Both examples for c1 and c2 are very simple. Indeed, these relationships are identified in very long parametric trees, considerably increasing the calculation of the dynamic facts.

IV. SQT-RS IN 5G GREEN ENVIRONMENTS

In this section, the steps taken to deploy SQT-RS to assess the Security and QoS tradeoff in 5G Green environments are described. The solution is tested in Section V taking into account the specific use case of relay selection in 5G scenarios. Different types of goals are selected, and the SQT returns recommendations for achieving the selected goals, given the facts extracted from the CPRM-based 5G Green system. The complete map of actions carried out in this section using the SQT-RS tool is shown in Figure 4.

The $CPRM_i$ to be evaluated is built based on the value of parameters selected by the user, which determine the type of relay used at a given time, according to the parameters taken from [4]. The instantiated model considers the behaviour when, in the environment, there are eavesdroppers or jammers. This information is taken from [19], [20], [21], [22].

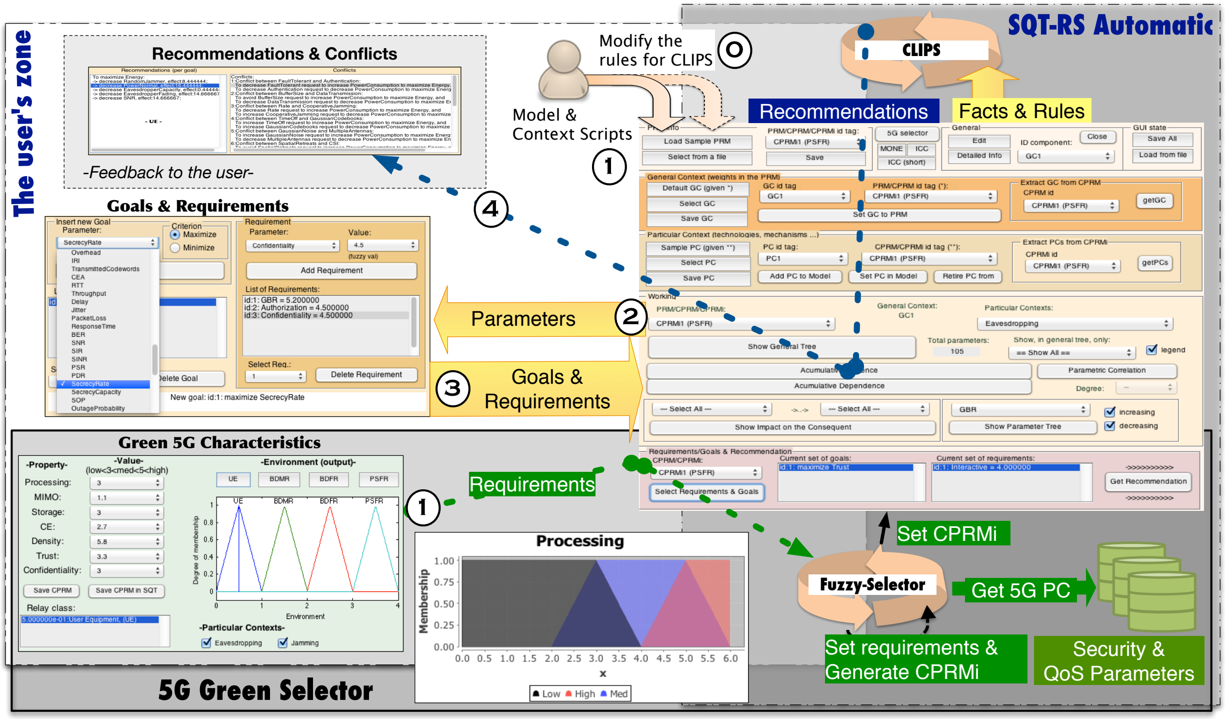


Figure 4. Deployment using 5G selector.

A. Automatic selection of CPRM-based 5G environment

SQT has been improved so as to provide a module to build, based on a set of requirements, $CPRM_i$ scripts specific to 5G Green scenarios (Figure 1). The SQT-5G Green module defines the input variables/parameters *Processing, MIMO, Storage, CE, Density, Trust and Confidentiality*, that are capabilities for relay classes in 5G scenarios according to [4]. The possible values for the different parameters, expressed as requirements to be satisfied or facts in the system, take fuzzy values given the membership (MS) functions trapezoidal *Low* $[0, 0, 3, 4]$, *Med* $[2, 3, 5, 6]$, and *High* $[4, 5, 6, 6]$. In the final system, there is a fuzzy-variable for each parameter defined as a requirement, and, by default, each variable (parameter) uses the same MS functions to map their values. See, for example, the values taken by MS functions for the parameter Processing in Figure 4.

These variables are inputs for 65 rules that characterise the 5G scenario. In particular, these scenarios are based on the relay class used: *User Equipment* (UE), *Battery-Dependent Mobile Relay* (BDMR), *Battery-Dependent Fixed Relay* (BDFR) and *Power-Supplied Fixed Relay* (PSFR) [4].

The final aim of this component, is to simplify the use of SQT. Based on the result/output (UE, BDMR, BDFR, PWFR), the CPRM-based system is generated, and the PCs shown in Table V are integrated. The result is then included in SQT-RS. As shown in Figure 1, four basic combinations (scripts) can be generated: CPRM-5GGreen (without PC added), CPRMi-5GGreen & PC1, CPRMi-5GGreen & PC2, or CPRMi-5GGreen & PC1 & PC2. Moreover, the user can change the value of the parameters inside the schemes, so these basic configurations can be adapted to the specific scenarios.

B. Description of the CPRM-based 5G Green environment

SQT-RS provides recommendations based on a set of parameters and their relationships defined as part of a CPRM-based system. Hence, a general description of the parameters to be considered in a 5G Green environment and the assumptions for the analysis are provided below.

1) CPRM-based 5G Green model: The set of parameters considered in the analysis, classified in layers, is shown in Table IV. This is a cross-layer classification based on abstract relationships between parameters. Hence, the parameters are not classified based on physical layers, but rather, on abstract layers [23]. For example, the *Secrecy Rate* can be considered as a physical security mechanism, however, in our classification, it is considered as part of the measurements layer because it is used as a measurement of the security at the physical layer in relay networks.

The selected parameters combine mobile platform parameters and relay network parameters. The aim of this selection is to provide a basic context with the definition of candidate parameters to be instantiated.

The weights for some parameters in Table IV are different, depending on the relay class and the selected policy according to [4]. The changes in the default values are indicated in Table IV, in parentheses just after the parameter involved. For example, UserExperience is targeted with a weight equal to 3 for UE relays, because it is more *relevant* in those scenarios where UEs are used. These changes in the weights are modelled through the GCs.

2) Particular contexts: The specific contexts considered are shown in Table V. In the following paragraphs, two specific contexts are added to the CPRM chosen in the previous step:

Table IV
Parameters for a Base Context in 5G Green

	High Level Requirements
Resource type	Guaranteed bit rate (GBR), non GBR (N-GBR).
Security	Authentication, authorisation, accounting, confidentiality, integrity, non repudiation, trust, privacy.
QoE	Conversational, Interactive, Streaming, Background, User Experience (UE=6, BDMR=4, BDFR=0, PSFR=0).
Characteristic	Complexity, fault tolerant (BDFR=4, PSFR=6), availability (BDFR=4, PSFR=6), reliability.
	Local Properties
Resource	Battery, Memory, Processing, Storage.
Performance	Node lifetime, power consumption.
Security	Anti-tampering, signature, encryption, Asymmetric Cryptography (AC), Symmetric Cryptography (SC), key generation, Reputation.
Characteristic	Mobility(UE=4, BDMR=6, BDFR=0, PSFR=0), relay class.
Threat	Misbehaviour (UE=3).
	Communication
Resource	Available time-slots, buffer size.
Performance	Packet size, signal strength, data transmission, transmission time, transmission power (PSFR=4), reception power, time on, time off, transmission capacity (PSFR=4), rate.
Security	collaborative jamming, Gaussian codebooks.
Characteristic	Multiple antennas, MIMO, successive relaying, half-duplex (HD), full-duplex (FD), decode and forward (DF), amplify-and-forward (AF), channel surfing, spatial retreats, Channel State Information (CSI) (BDFR=3, PSFR=6) availability, multimode.
Consequence	Retransmission, congestion, overhead, inter-relay interference (IRI).
	Measurements
Performance	Max rate, min rate, transmitted codewords, Channel Estimation Accuracy (CE) , RTT, throughput, delay, jitter, packet loss, response time, bit-error rate (BER), Signal-to-noise ratio (SNR), Signal-to-interference ratio (SIR), Signal-to-interference-plus-noise ratio (SINR), packet sent ratio (PSR), packet delivery ratio (PDR).
Security	Secrecy rate, secrecy capability, secrecy outage probability (SOP).
Consequence	Outage probability.
	Environment
Characteristic	Density, participants, diversity, noise, channel symmetry, network lifetime, multi-path fading, eavesdropper fading, Handover.
Consequence	Error probability.
Threat	Denial of Service (DoS), Eavesdropping, Jamming.

Table V
Weights w_d for Relationships in the PCs

	Dependence			
Context	Antecedent	Rel.	Consequent	w_d
Eavesdropping	EavesdropperFading	c	SecrecyRate	1
	EavesdroppingFading	nc	Eavesdropping	1
(E)	EavesdroppingCapacity	c	Eavesdropping	1
	EavesdropperCapacity	$\neg c$	SecrecyCapacity	1
	ConstantJammer	+	DoS	4
	ConstantJammer	$\neg c$	PDR	3
	DeceptiveJammer	+	DoS	4
Jamming	DeceptiveJammer	+	TimeOn	4
	RandomJammer	+	DoS	2
	ReactiveJammer	+	DoS	3
	ReactiveJammer	+	TimeOn	3
	ReactiveJammer	i-	PSR	0
(J)	ReactiveJammer	$\neg c$	PDR	5
	Jamming	c	PowerJamming	1
	PowerJamming	$\neg c$	SecrecyCapacity	1
	PowerJamming	$\neg c$	TransmissionCapacity	3

Eavesdropping (E) and Jamming (J). Note that, in Table IV, Eavesdropping and Jamming are parameters of type *Threat* at the layer *Environment*.

In the Eavesdropping context, new parameters are added to enhance the information in the models with information typically considered in eavesdropping scenarios [19], [20]. For example, the fading in the eavesdropper's channel determine the secrecy rate. As this is a characteristic with additional relationships (due to the eavesdropper's role), then, the parameter EavesdropperFading is added as an instance of Fading. Moreover, a new parameter called NormalFading is added to inherit the default behaviour of the parameter Fading (inheritance process described in [7]). This parameter is included to consider those cases where the eavesdropper is not affecting the parameter Fading. In the same way, the eavesdropper's capacity produces the opposite effect on the secrecy capacity [20] with respect to the normal behaviour, as defined for the Transmission Capacity. Therefore, the parameter NormalCapacity is defined to inherit the default behaviour of Capacity. In both cases, these parameters do not define new relationships (and for this reason are not shown in Table V), because the only purpose is to maintain the default behaviour of the instantiated parameters and therefore to be able for comparing the default behaviour with the new one.

Furthermore, the specific context for Jamming (J), is built based on the information given in [22], where a discussion on how to identify different types of jammers (constant, deceptive, random and reactive) based on the effect on the performance parameters *Packet Delivery Rate* (PDR) and *Packet Sent Ratio* (PSR) is provided. PDR is calculated as the number of packages received from the total number of packets sent. Therefore, it is a measure of the boundary of the channel. Contrarily, the PSR is a measure of packets sent by a legitimate sender. The authors explain when, depending on the type of jamming, it is better to use PDR or PSR to identify possible jammers.

In addition, according to [20], the channel capacity under jamming decreases based on the jammer's transmit power. To consider this effect, the parameter PowerJamming is added in the PC (J) to inherit the general behaviour of TransmissionPower and add the behaviour relative to the jamming scenario. As in (E), an additional parameter was added to maintain the behaviour of TransmissionPower by default. Besides, (E) or (J), when new properties are added to a parameter defined in a CPRM, it is necessary to add the relationship between this parameter and the new one. This is done in (J) to PowerJamming, where the relationship $PowerJamming \xrightarrow{\neg c} TransmissionCapacity$ is added. This is because PowerJamming inherits the behaviour of Power, so, by default, PowerJamming effects the instances of TransmissionCapacity positively. To prevent this behaviour, a negative complete ($\neg c$) relationship is introduced. Note that, when we do this, the model does not show the behaviour of the jammer, but rather, it concentrates on the effect of the jammer in the model. Moreover, the eavesdropper capacity is considered in the model to evaluate the effect of eavesdropping on the model. This requirement is related to the availability of global state information.

3) Goals: The analysis is based on the selection of two goals. First, the parameter secrecy rate is selected to be maximised, given its relevance for this particular use case, according to the literature. In fact, other parameters such as secrecy capacity and *secrecy outage probability* (SOP) used as security metrics in several previous approaches can be defined based on the secrecy rate [4]. So, as shown in Figure 5, when this parameter is increased, the probability for eavesdropping

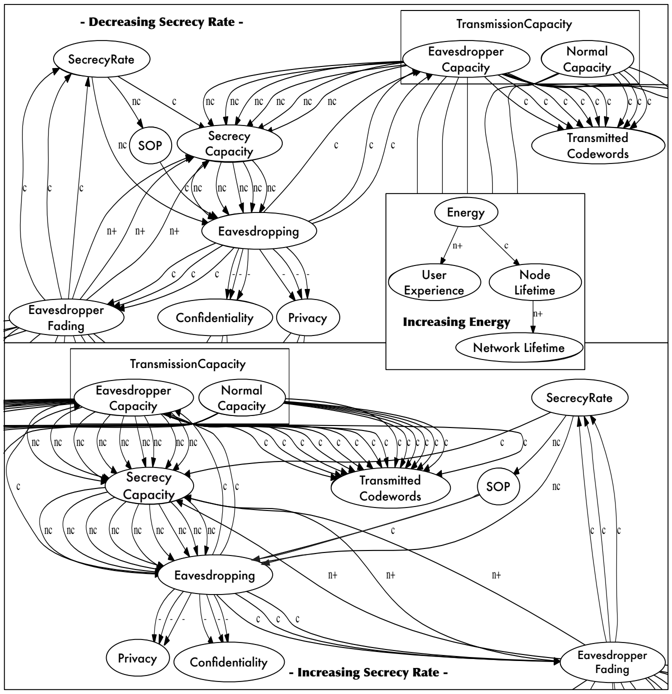
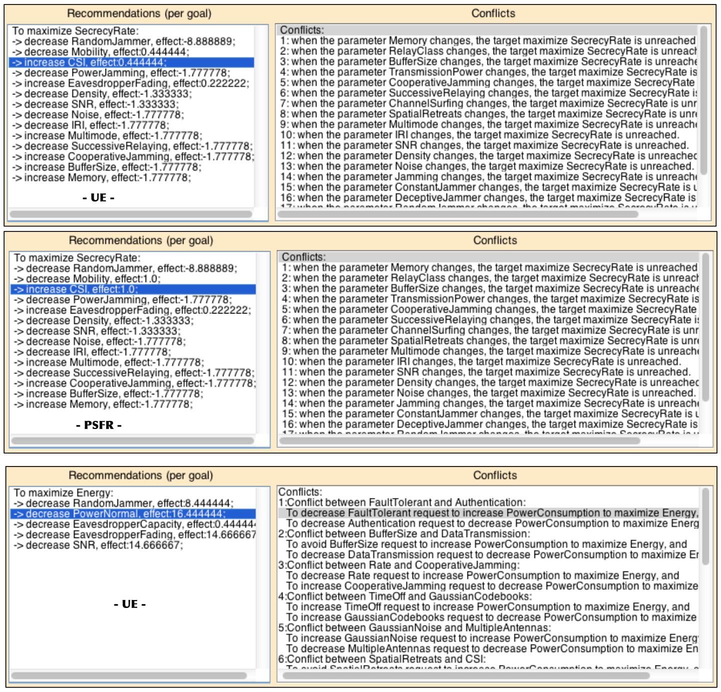


Figure 5. Sections of particular parametric trees.



```
To maximize SecrecyRate:
-> decrease RandomJammer, effect:-8.888889;
-> decrease Mobility, effect:0.444444;
-> increase CSI, effect:0.444444;
-> decrease PowerJamming, effect:-1.777778;
-> increase EavesdropperFading, effect:0.222222;
-> decrease Density, effect:-1.333333;
-> decrease SNR, effect:-1.333333;
-> decrease Noise, effect:-1.777778;
-> decrease IRI, effect:-1.777778;
-> increase Multimode, effect:-1.777778;
-> decrease SuccessiveRelaying, effect:-1.777778;
-> increase CooperativeJamming, effect:-1.777778;
-> increase BufferSize, effect:-1.777778;
-> increase Memory, effect:-1.777778;
```

```
Conflicts:
1: when the parameter Memory changes, the target maximize SecrecyRate is unreached
2: when the parameter RelayClass changes, the target maximize SecrecyRate is unreach
3: when the parameter BufferSize changes, the target maximize SecrecyRate is unreache
4: when the parameter TransmissionPower changes, the target maximize SecrecyRate is
5: when the parameter CooperativeJamming changes, the target maximize SecrecyRate
6: when the parameter SuccessiveRelaying changes, the target maximize SecrecyRate i
7: when the parameter ChannelSurfing changes, the target maximize SecrecyRate is unr
8: when the parameter SpatialRetreats changes, the target maximize SecrecyRate is unr
9: when the parameter Multimode changes, the target maximize SecrecyRate is unreache
10: when the parameter IRI changes, the target maximize SecrecyRate is unreached.
11: when the parameter SNR changes, the target maximize SecrecyRate is unreached.
12: when the parameter Density changes, the target maximize SecrecyRate is unreachec
13: when the parameter Noise changes, the target maximize SecrecyRate is unreached.
14: when the parameter Jamming changes, the target maximize SecrecyRate is unreache
15: when the parameter ConstantJammer changes, the target maximize SecrecyRate is u
16: when the parameter DeceptiveJammer changes, the target maximize SecrecyRate is
```

```
To maximize SecrecyRate:
-> decrease RandomJammer, effect:-8.888889;
-> decrease Mobility, effect:1.0;
-> increase CSI, effect:1.0;
-> decrease PowerJamming, effect:-1.777778;
-> increase EavesdropperFading, effect:0.222222;
-> decrease Density, effect:-1.333333;
-> decrease SNR, effect:-1.333333;
-> decrease Noise, effect:-1.777778;
-> decrease IRI, effect:-1.777778;
-> increase Multimode, effect:-1.777778;
-> decrease SuccessiveRelaying, effect:-1.777778;
-> increase CooperativeJamming, effect:-1.777778;
-> increase BufferSize, effect:-1.777778;
-> increase Memory, effect:-1.777778;
```

```
Conflicts:
1: when the parameter Memory changes, the target maximize SecrecyRate is unreached
2: when the parameter RelayClass changes, the target maximize SecrecyRate is unreach
3: when the parameter BufferSize changes, the target maximize SecrecyRate is unreache
4: when the parameter TransmissionPower changes, the target maximize SecrecyRate is
5: when the parameter CooperativeJamming changes, the target maximize SecrecyRate
6: when the parameter SuccessiveRelaying changes, the target maximize SecrecyRate i
7: when the parameter ChannelSurfing changes, the target maximize SecrecyRate is unr
8: when the parameter SpatialRetreats changes, the target maximize SecrecyRate is unr
9: when the parameter Multimode changes, the target maximize SecrecyRate is unreache
10: when the parameter IRI changes, the target maximize SecrecyRate is unreached.
11: when the parameter SNR changes, the target maximize SecrecyRate is unreached.
12: when the parameter Density changes, the target maximize SecrecyRate is unreachec
13: when the parameter Noise changes, the target maximize SecrecyRate is unreached.
14: when the parameter Jamming changes, the target maximize SecrecyRate is unreache
15: when the parameter ConstantJammer changes, the target maximize SecrecyRate is u
16: when the parameter DeceptiveJammer changes, the target maximize SecrecyRate is
```

```
To maximize Energy:
-> decrease RandomJammer, effect:8.444444;
-> decrease PowerNormal, effect:16.444444;
-> decrease EavesdropperCapacity, effect:0.44444
-> decrease EavesdropperFading, effect:14.666667
-> decrease SNR, effect:14.666667;
```

```
Conflicts:
1:Conflict between FaultTolerant and Authentication:
  To decrease FaultTolerant request to increase PowerConsumption to maximize Energy,
  To decrease Authentication request to decrease PowerConsumption to maximize Energ
2:Conflict between BufferSize and DataTransmission:
  To avoid BufferSize request to increase PowerConsumption to maximize Energy, and
  To decrease DataTransmission request to decrease PowerConsumption to maximize Er
3:Conflict between Rate and CooperativeJamming:
  To decrease Rate request to increase PowerConsumption to maximize Energy, and
  To increase CooperativeJamming request to decrease PowerConsumption to maximize
4:Conflict between TimeOff and GaussianCodebooks:
  To increase TimeOff request to increase PowerConsumption to maximize Energy, and
  To increase GaussianCodebooks request to decrease PowerConsumption to maximize
5:Conflict between GaussianNoise and MultipleAntennas:
  To increase GaussianNoise request to increase PowerConsumption to maximize Energ
  To decrease MultipleAntennas request to decrease PowerConsumption to maximize En
6:Conflict between SpatialRetreats and CSI:
```

Figure 6. SecrecyRate - UE and PSFR, Energy - UE.

decreases, and then the confidentiality and privacy increases. Note that an alternative interpretation could be that when eavesdropping occurs, the secrecy rate will probably be poor. However, this depends on the type of eavesdropper and the properties defined. So, in this case, we have a protective outlook, in which the probability of misbehaviour decreases or is prevented when the security is improved.

Although the parametric trees for the secrecy rate (Figure 5) are similar in both cases (∇ and Δ), the relationships from Confidentiality and Privacy to UserExperience are not considered in the case of increasing the parameters Confidentiality and Privacy. This is because it has been considered that a security failure in such terms may affect the UserExperience much more than the correct performance of the system, which, for many users, is considered normal. An alternative approach is to use different weights for the cases where, an improvement in the security properties is not directly perceived by the user but the deterioration is.

The maximisation of Energy is also considered. In this case, as energy is close to being a leaf node, this parameter will not affect the large number of parameters behind it. However, it does affect the node's lifetime, which is critical for the survivability of the node, and, therefore, given the ad-hoc nature of future networks, and moreover, relay networks, it is fundamental for the lifetime of relay nodes that are battery-dependent.

V. Analysis

In this section, the recommendations for the different goals based on the contexts are discussed.

A. Recommendations and Conflicts

The parameters Secrecy Rate and Energy are the chosen goals using SQT-RS to assess Security and QoS tradeoff in 5G Green scenarios. These parameters have different behaviours, and, therefore, the recommendations/ goals will also be different. Moreover, as different types of relays define different relevance for the parameters, the results given for the different scenarios, vary regarding the final effect that the recommendation produces.

1) SecrecyRate: Figure 6 shows the relevant parameters for maximising SecrecyRate. In this case, a reduced group of parameters are capable of performing changes in it, given our definition of the models. The list of parameters in the recommendation are without order because in this case the ordering of subgoals is avoided.

As one of the main approaches to maximise the secrecy rate is to gain advantage over the eavesdropper through optimal relay selection, it is expected that the behaviour for CPRM-based non-limited relays improve the secrecy rate at the expense of increasing the value of the parameters at the communication layer. That means that the best improvements in secrecy rate can be made by the PSFR relays. Moreover, the fixed relays (PSFR and BDFR) are not mobile nodes and thus, global CSI can be acquired in time to identify the quality of the channel when the secrecy rate is calculated, unlike UEs and BDMRs. Also, for the case of UEs a serious concern is that misbehaviour is likely to occur, thus raising trust issues.

2) Energy: In Figure 6, the relevant parameters for maximising Energy are shown for UE without loss of generality. The value of the relevant parameters to Energy (left-hand side of the window) are quite similar, so the recommendations for that are similar too. However, although PSFR is not battery-dependent, the relevance of this parameter is higher than 0, because in Green networks it is a significant requirement. In our model, the principal parameter that affects Energy is modelled as PowerConsumption, and the instance PowerNormal is the most relevant. The EavesdropperFading parameter has been related Energy because, in the recommendation, it is the instance of Fading that maximises the goal. Moreover, there is a large number of defined conflicts (right side of the window). This is because in the current version, all the conflicts between the intermediate parameters are listed. For example, the conflict between FaultTolerant and Authentication, which occurs when FaultTolerant is decreased. This behaviour is reasonable, because FaultTolerant requires the deployment of additional mechanisms that take measurements and implement protocols to react to diverse events in real time. So, while decreasing FaultTolerant, Energy increases but, as there are additional mechanisms that will not be applied, this is not always desirable.

As can be observed in Figure 6, there is a long list of conflicts that affect the PowerConsumption and Energy. In its current form, the list of conflicts is a log that shows additional information to the recommendations. Thus, one may observe that although in the list of recommendations PowerNormal is considered as the most representative instance to maximise Energy, in the list of conflicts the parameter that appears is PowerConsumption, because its behaviour is more general. Furthermore, when a parameter defines the same behaviour for several instances, the list of conflicts can be summarised using the instantiated parameters instead of using the instances.

B. *Final Remarks*

In what follows, additional considerations regarding the models used in the analysis for 5G Green networks are presented. The aim of this section is to provide an overview on some of the issues that are considered in the design of CPRM-based systems. These are illustrated using some of the design issues in the definition of the parametric sets used in the analysis.

1) User-oriented Approach: In this classification, the UE and BDMR have a strong effect on the user's experience, and therefore, the relevance of these parameters increases with respect to the rest of the cases.

One interesting issue found here, is that when mobility is influenced, the network lifetime always decreases. However, mobility is not directly related to this parameter, but rather it is related to the parameters of the network that affect the network lifetime and also, the reaction to attacks, such as moving the legitimate nodes to gain advantage over the malicious nodes (e.g. avoid jammers or eavesdroppers). So, the parameter - network lifetime - represents a conflict for any parameter which affects mobility as an intermediary parameter. Therefore, this behaviour particularly affects BDMR, where the parameter's mobility becomes much more relevant, because the devices have this capability.

2) Resource Independence: The types of relays chosen have their own characteristics that, provided in the tool, give us information about the different behaviours based on the relevance of the selected parameters. In greater detail, when PSFR is modelled, the user's experience is not considered, because the user is the final user of the infrastructure, and not the operator, and so, the user's experience in the UE's scenario should be more relevant than the PSFR.

Therefore, the PSFR takes advantage not only of the independence of the user's perception, but also of the fact that resources for defense against the different attacks are not as limited as for the rest of the relays. However, network performance and availability are significant at this point. When a fixed base station is a target, the mobility of the base station to take advantage of the signal, is not an option.

3) Discussion about the Relationships: As mentioned, SQT-RS is a knowledge-based system. Specifically, SQT-RS depends on the relationships defined in the CPRM-based environment. Therefore, our decisions about what relationships should be considered have a decisive impact on the final results. This should be carefully considered.

a) Eavesdropping: For example, one of the decisions that should be discussed is that of the relationships defined between SecrecyRate and Eavesdropping. One may observe in Figure 5, that SecrecyRate influences Eavesdropping but the opposite relationship is not included. This is due to the behaviour between the parameters in (E). Two points should be considered here:

1) The relationship from Eavesdropping to EavesdropperFading implies that when there is eavesdropping activity then eavesdropper fading is present. However, this interpretation entails the risk of considering the performance in the channel of the eavesdropper as not good, and this is not necessarily true in all cases.
2) The interpretation of EavesdroppingFading and EavesdroppingCapacity changes depending on their placement in the relationships. In our analysis, it has been assumed that both parameters influence Eavesdropping, so both are in the antecedent. Although the existence of Eavesdropping implies that there is specific fading and capacity, the interpretation chosen allows the eavesdropper's behaviour to be modelled given these parameters.

In greater detail, related to (1), as the increase of the EavesdroppingFading degrades the reception of the eavesdropper, this is considered as an improvement for SecrecyRate. Therefore, to relate Eavesdropping and SecrecyRate, the relationship between these parameters should define a higher weight than the relationship between EavesdropperFading and SecrecyRate.

b) Jamming: As it has been detailed, PowerJamming redefines the relationship with TransmissionCapacity, not only the weight, but also, the instance redefines the operation with TransmissionCapacity, which by default is c due to the relationship between TransmissionPower and TransmissionCapacity. However, this redefinition causes the following chain of dependencies:

1) Δ PowerJamming triggers a ∇ in TransmissionCapacity. TransmissionCapacity is instantiated, so this effect is propagated to the instances EavesdroppingCapacity and NormalCapacity. This is logical, because jamming affects both normal devices and eavesdroppers.

2) When EavesdroppingCapacity is decreased, Eavesdropping is also decreased, because they are related to a complete relationship *c*. When Eavesdropping decreases, SecrecyRate increases, because if there are not eavesdroppers, then SecrecyRate is maximum.

However, SecrecyRate cannot be maximum if it is imposible to send information because the network has collapsed due to Jamming. Therefore, environmental conditions have to be related to SecrecyRate and therefore decrease the positive impact on SecrecyRate. In our case, Rate is directly related to SecrecyRate using an inverse positive relationship: when Rate decreases, SecrecyRate also decreases.

4) Discussion about the Weights: Prior to the analysis of the results, the set of parameters and their relationships have to be thoroughly tested in order to model the behaviour of a 5G Green relay system. This entails different tests for identifying general inconsistencies given by the propagation of the effects through the parametric tree. When the behaviour of the model with the parameters in the basic set is reasonable (e.g., it is assumed that the parameter Energy increases/decreases when the parameter PowerConsumption decreases/increases), the models are built using the basic parameters' set and adding the new specific parameters and relationships. Then, the recommendations provided by SQT-RS can be evaluated.

VI. Conclusions and Future Work

In this paper, the steps taken to deploy SQT-RS to assess in the Security and QoS tradeoff in 5G Green environments have been described. With this aim, the module SQT-5G has been provided to define the behaviour of Green 5G-based CPRM systems based on the context selected by the user, considering the particular case of relay networks. SQT-RS generates the facts to be processed by an expert system dynamically based on the current behaviour of the systems generated by SQT-5G, and the set of goals and requirements selected by the user. The result of this process is a set of recommendations and conflicts to satisfy the goals. As a future work, the idea behind SQT-RS can be adapted to be implemented in resource-constrained nodes, perhaps avoiding some characteristics (e.g., GUI), and delegating part of the control/decisions about the configuration to powerful nodes in the network. It is also interesting to increase the number of parameters that can be analysed in a 5G Green context. Finally, an interesting feature of SQT-RS is that it can be enhanced to provide recommendations considering different user profiles without changes in the core of the definition of the model, by adapting the recommendations provided by the rules.

References

[1] M. Olsson, C. Cavdar, P. Frenger, S. Tombaz, D. Sabella, and R. Jantti, "5green: Towards green 5g mobile networks," in *Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on*. IEEE, 2013, pp. 212–216.

[2] J. Laneman, D. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3062–3080, 2004.

[3] N. Nomikos, T. Charalambous, I. Krikidis, D. Skoutas, D. Vouyioukas, and M. Johansson, "Buffer-aided successive opportunistic relaying with inter-relay interference cancellation," in *Personal, Indoor and Mobile Radio Communications, 2013. PIMRC 2003. 24th IEEE Proceedings on*. IEEE, 2013, pp. 1316–1320.

[4] N. Nomikos, A. Nieto, P. Makris, D. Skoutas, D. Vouyioukas, P. Rizomiliotis, J. Lopez, and C. Skianis, "Relay selection for secure 5g green communications," *Springer Telecommunication Systems*, pp. 1–35, 2014.

[5] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 16–28, 2013.

[6] A. Imran, A. Zoha, and A. Abu-Dayya, "Challenges in 5g: how to empower son with big data for enabling 5g," *Network, IEEE*, vol. 28, no. 6, pp. 27–33, 2014.

[7] A. Nieto and J. Lopez, "A context-based parametric relationship model (cprm) to measure the security and qos tradeoff in configurable environments," in *IEEE International Conference on Communications (ICC)*. IEEE, 2014, pp. 755–760.

[8] Z. Bojković and B. Bakmaz, "Quality of service and security as frameworks toward next-generation wireless networks," in *Proceedings of the 6th WSEAS international conference on Automation & information*, 2005, pp. 352–357.

[9] A. Nieto and J. Lopez, "Security and qos tradeoff recommendation system (sqt-rs) for dynamic assessing cprm-based systems," in *10th ACM International Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet'14)*. ACM, 2014, pp. 25–32.

[10] I. Chih-Lin, C. Rowell, S. Han, Z. Xu, G. Li, and Z. Pan, "Toward green and soft: a 5g perspective." *IEEE Communications Magazine*, vol. 52, no. 2, pp. 66–73, 2014.

[11] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-device communication in 5g cellular networks: challenges, solutions, and future directions," *Communications Magazine, IEEE*, vol. 52, no. 5, pp. 86–92, 2014.

[12] V. C. Leung, T. Taleb, M. Chen, T. Magedanz, L.-C. Wang, and R. Tafazolli, "Unveiling 5g wireless networks: emerging research advances, prospects, and challenges [guest editorial]," *Network, IEEE*, vol. 28, no. 6, pp. 3–5, 2014.

[13] H. Abou-Zeid and H. S. Hassanein, "Toward green media delivery: location-aware opportunities and approaches," *Wireless Communications, IEEE*, vol. 21, no. 4, pp. 38–46, 2014.

[14] X. Zhang, W. Cheng, and H. Zhang, "Heterogeneous statistical qos provisioning over 5g mobile wireless networks," *Network, IEEE*, vol. 28, no. 6, pp. 46–53, 2014.

[15] N. Cordeschi, M. Shojafar, D. Amendola, and E. Baccarelli, "Energy-efficient adaptive networked datacenters for the qos support of real-time applications," *The Journal of Supercomputing*, pp. 1–31, 2014.

[16] R. Guerzoni, R. Trivisonno, and D. Soldani, "Sdn-based architecture and procedures for 5g networks," in *5G for Ubiquitous Connectivity (5GU), 2014 1st International Conference on*. IEEE, 2014, pp. 209–214.

[17] L. Suomalainen, E. Nikkhouy, A. Y. Ding, and S. Tarkoma, "Open source platforms, applications and tools for software-defined networking and 5g research," 2014.

[18] C. Giarratano, "Clips: C language integrated production system," *CLIPS users guide-version*, vol. 6, 1993.

[19] S. Yuan and D. Stewart, "Protection of optical networks against inter-channel eavesdropping and jamming attacks," in *Computational Science and Computational Intelligence (CSCI), 2014 International Conference on*, vol. 1. IEEE, 2014, pp. 34–38.

[20] Q. Zhu, W. Saad, Z. Han, H. V. Poor, and T. Basar, "Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach," in *MILITARY COMMUNICATIONS CONFERENCE, 2011-MILCOM 2011*. IEEE, 2011, pp. 119–124.

[21] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: defenses against wireless denial of service," in *Proceedings of the 3rd ACM workshop on Wireless security*. ACM, 2004, pp. 80–89.

[22] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *Network, IEEE*, vol. 20, no. 3, pp. 41–47, 2006.

[23] A. Nieto and J. Lopez, "A model for the analysis of qos and security tradeoff in mobile platforms," *Mobile Networks and Applications*, vol. 19, no. 1, pp. 64–78, 2014.