Semiring-based Specification Approaches for Quantitative Security

CONFERENCE PAPER · MARCH 2015

DOI: 10.4204/EPTCS.194.7

Ilaria Matteucci

Italian National Research Council

Francesco Santini

Università degli Studi di Perugia

Semiring-based Specification Approaches for Quantitative Security[*]

Fabio Martinelli
IIT-CNR, Pisa, Italy
fabio.martinelli@iit.cnr.it

Ilaria Matteucci
IIT-CNR, Pisa, Italy
ilaria.matteucci@iit.cnr.it

Francesco Santini
IIT-CNR, Pisa, Italy
francesco.santini@iit.cnr.it

Our goal is to provide different semiring-based formal tools for the specification of security requirements: we quantitatively enhance the *open-system* approach, according to which a system is partially specified. Therefore, we suppose the existence of an unknown and possibly malicious agent that interacts in parallel with the system. Two specification frameworks are designed along two different (but still related) lines. First, by comparing the behaviour of a system with the expected one, or by checking if such system satisfies some security requirements: we investigate a novel approximate behavioural-equivalence for comparing processes behaviour, thus extending the *Generalised Non Deducibility on Composition* (GNDC) approach with scores. As a second result, we equip a modal logic with *semiring* values with the purpose to have a score related to the satisfaction of a formula that specifies some requested property. Finally, we generalise the classical partial model-checking function, and we name it as *quantitative partial model-checking* in such a way to point out the necessary and sufficient conditions that a system has to satisfy in order to be considered as secure, with respect to a fixed security/functionality threshold-value.

1 Introduction

The considerable amount of trust and decentralisation, coming with today's software systems, demands for a rigorous security analysis. Unfortunately, security is frequently in conflict with the functionality and performance requirements of a system, making 100% security an impossible or overly expensive goal to be accomplished. For instance, functional requirements add to the picture costs, execution times, and rates. Therefore, the relevant question is not whether a system is secure, but rather how much security it provides under such "soft" constraints. Instead of a plain yes/no answer, quantitative levels of security can express different degrees of protection, and allow a security expert to reason about the trade-off between security and conflicting requirements (*e.g.*, on performance). Quantitative security analysis [21] has been already applied, *e.g.*, to name a few, for quantifying the side-channel leakage in cryptographic algorithms, for capturing the loss of privacy in statistical data analysis or information flows, and for quantifying security in anonymity networks.

Improving a quantitative security-analysis requires different tools for the rigorous development of practical systems, and an extended formal foundation for the management of security risks. Here we focus on the latter task. The goal of this paper is to move from a qualitative interpretation of security to a quantitative one. The basic ingredients in our "recipe" are c-semirings [8, 6] (or simply "semirings" in the following) and the *Generalised Process Algebra* (*GPA*) [10], a quantitative process-algebra where actions are labelled with a value taken from a semiring. Therefore, we use GPA to model processes with quantitative aspects: different semiring instantiations can parametrically model different cost-metrics. In order to formalise security-properties of GPA processes, we provide two different approaches.

[*]This work has been partially supported by PRIN 2010XSEMLC "Security Horizons" and ARTEMIS J.U. SESAMO.

Submitted to:
QAPL 2015

The **first approach** consists in providing several definitions of quantitative behavioural-equivalencies in such a way to extend with quantities the family of security properties that can be expressed in *Generalised Non Deducibility on Composition* (*GNDC*) [17]. The GNDC schema is a uniform approach for defining security properties derived from the *Non Deducibility on Composition* (NDC) properties [19, 15]. The GNDC scheme uniformly expresses many security properties as, *e.g.*, fault tolerance properties (*fail stop, fail silent, fail safe* and *fault tolerant* behaviour, *e.g.*, [22]) or, also, many security properties of cryptographic protocols as, *e.g.*, *secrecy*, *authentication*, *integrity*, etc. [16]. Hence, we formalise the system through quantitative observational relations. We introduce the notion of *quantitative trace-equivalence*, and we recall the definition of *quantitative bisimulation* given in [27]. Furthermore, we extend both these relations by considering an approximate version of them: the ε-equivalence. By using these equivalence relations, we can compare and specify different security properties, as a quantitative extension of NDC and bisimulation-based NDC properties (BNDC) [19, 15].

In the **second approach** we present in this paper, we first introduce a semiring-based extension of the classical *Hennessy-Milner Logic* (named *c-HM* Logic) as a means to quantitatively measure the satisfaction of a given formula: its truth value can now be not only true/false, but a numeric value as well (*e.g.*, 50% or 3€). Note that by exploiting the boolean semiring (i.e., $\langle\{false, true\}, \vee, \wedge, false, true\rangle$) we can still enforce yes/no only requirements. Hence, we use c-HM Logic in the frame of *Partial Model Checking* (*PMC*) [2]. Classical *Model Checking* (*MC*) involves using verification tools to exhaustively search in a process/protocol specification for all the execution sequences with some desired properties. PMC focuses this verification on part of a system only: the main advantage is to perform a full analysis while avoiding the combinatorial explosion of the state space.

In security, the PMC function has been often used to point out necessary and sufficient constraints on the unspecified/unknown part of a system that is supposed to show a malicious behaviour. Hence, a controller program is required to ensure the correct behaviour of the whole system, comprehensive of the attacker [24]. In a quantitative scenario, we associate the notion of satisfiability of a logic formula with the security/functionality level of a system. Once we set a *satisfiability threshold* $t \in K$, if the system quantitatively satisfies a security requirement ϕ with a value k worse than t, then we can state that the investigated system is not quantitatively secure.

The paper is structured as follows. In Sec. 2 we recall c-semiring algebraic structures and GPAs. In Sec. 3 we introduce our first approach, which aims at comparing a system behaviour with the expected one: we adopt both trace and bisimulation equivalence. Hence, we rephrase them as approximate relations, in order to include “close”-enough processes, where close is related to a threshold-score ε. In this way, we are able to specify some security aspects formalised as a quantitative GNDC schema. In Sec. 4 we describe security properties via a semiring-based modal logic (i.e., c-HM), and in Sec. 5 we define a QPMC function with the purpose to point out the necessary and sufficient conditions each subsystem has to satisfy for guaranteeing such requirements. Finally, Sec. 6 summarises the related work in literature, and Sec. 7 wraps up the paper with conclusions and proposes some future work.

2 Background

In this section we recall the necessary fundamental notions about c-semirings [8, 6] and *Generalised Process Algebra* [10], a quantitative process-algebra based on semirings.

2.1 Semirings

Definition 2.1 (semiring [20])**.** *A commutative semiring is a five-tuple $\mathbb{K} = \langle K, +, \times, \bot, \top \rangle$ such that K is a set, $\top, \bot \in K$, and $+, \times : K \times K \to K$ are binary operators making the triples $\langle K, +, \bot \rangle$ and $\langle K, \times, \top \rangle$ commutative monoids (semigroups with identity), satisfying*

- *(distributivity) $\forall a, b, c \in K . a \times (b + c) = (a \times b) + (a \times c)$.*
- *(annihilator) $\forall a \in A . a \times \bot = \bot$.*

Proposition 2.1 (absorptive semirings [20])**.** *Let $\mathbb{K}$ be a commutative semiring. Then these two properties are equivalent:*

- *(absorptiveness) $\forall a, b \in K . a + (a \times b) = a$.*
- *($\top$ absorbing element of $+$) $\forall a \in K . a + \top = \top$.*

Absorptive semirings are referred also as *simple*, and their $+$ operator is necessarily idempotent [20, Ch. 1, pp. 14]. Semirings where $+$ is idempotent are called as *dioids*.

Definition 2.2 (c-semiring [8])**.** *C-semirings are commutative and absorptive semirings. Therefore, c-semirings are dioids where $\top$ is an absorbing element for $+$.*

The idempotency of $+$ leads to the definition of a partial ordering $\leq_K$ over the set K (K is a poset). Such partial order is defined as $a \leq_K b$ if and only if $a + b = b$, and $+$ becomes the *least upper bound* (*lub*, or $\sqcup$) of the lattice $\langle K, \leq_K \rangle$. This intuitively means that b is "better" than a. As a consequence, we can use $+$ as an optimisation operator and always choose the best available solution.

Some more properties can be derived on c-semirings [8]: *i)* both $+$ and $\times$ are monotone over $\leq_K$, *ii)* $\times$ is intensive (i.e., $a \times b \leq_K a$), iii) $\times$ is closed (i.e., $a \times b \in K$), and *iv)* $\langle K, \leq_K \rangle$ is a complete lattice. $\bot$ and $\top$ are respectively the bottom and top elements of such lattice. When also $\times$ is idempotent, *i)* $+$ distributes over $\times$, *ii)* $\times$ is the *greater lower bound* (*glb*, or $\sqcap$) of the lattice, and *iii)* $\langle K, \leq_K \rangle$ is a distributive lattice.

Semirings and c-semirings have been often adopted in Computer Science and Operation Research as a very simple but very expressive optimisation structure [30]. Some c-semiring instances are: *boolean* $\langle \{F, T\}, \vee, \wedge, F, T \rangle$[1], *fuzzy* $\langle [0,1], \max, \min, 0, 1 \rangle$, *bottleneck* $\langle \mathbb{R}^+ \cup \{+\infty\}, \max, \min, 0, \infty \rangle$, *probabilistic* $\langle [0,1], \max, \hat{\times}, 0, 1 \rangle$ (known as the Viterbi semiring), *tropical* $\langle \mathbb{N} \cup \{+\infty\}, min, \hat{+}, +\infty, 0 \rangle$. Capped operators stand for their arithmetic equivalent.

Although c-semirings have been historically used as monotonic structures where to aggregate costs (and find best solutions), the need of removing values has raised in local consistency algorithms and non-monotonic algebras using constraints (eg [6]). A solution comes from *residuation theory* [9], a standard tool on tropical arithmetics that allows for obtaining a division operator via an approximate solution to the equation $b \times x = a$.

Definition 2.3 (division [6])**.** *Let $\mathbb{K}$ be a tropical semiring. Then, $\mathbb{K}$ is residuated if the set $\{x \in K \mid b \times x \leq a\}$ admits a maximum for all elements $a, b \in K$, denoted as $a \div b$.*

Since a complete[2] dioid is also residuated, we have that all the classical instances of a c-semiring presented above are residuated, i.e., each element in K admits an "inverse", which is unique in case $\leq_K$ is a total order. For instance, the unique "inverse" $a \div b$ in the weighted semiring is defined as follows:

$$a \div b = \min\{x \mid b \hat{+} x \geq a\} = \begin{cases} 0 & \text{if } b \geq a \\ a \hat{-} b & \text{if } a > b \end{cases}$$

[1] Boolean c-semirings can be used to model crisp problems.

[2] $\mathbb{K}$ is complete if it is closed with respect to infinite sums, and the distributivity law holds also for an infinite number of summands [6].

Definition 2.4 (unique invertibility [6]). *Let $\mathbb{K}$ be an absorptive, invertible semiring. Then, $\mathbb{K}$ is uniquely invertible iff it is cancellative, i.e., $\forall a,b,c \in A.(a \times c = b \times c) \wedge (c \neq 0) \Rightarrow a = b$.*

Note that since all the previously listed semirings (*e.g.*, tropical and fuzzy) are cancellative, they are uniquely invertible as well. Furthermore, it is also possible to consider several optimisation criteria at the same time: the cartesian product of semirings is still a semiring. Clearly, in this case the ordering induced by $+$ is partial, *e.g.*, when we have $\langle k_1, k_2 \rangle$ and $\langle k_3, k_4 \rangle$, and $k_1 \leq k_3$ while $k_2 \geq k_4$.

2.2 Generalised Process Algebra

In a *quantitative process*, observable transitions are labelled with some value associated with a step in the behaviour of a system. In GPA [10] the authors use semirings to model two fundamental modes of composing observable behaviour, either by combination of different traces, or by sequential composition. Process algebras are simple languages with precise mathematical semantics, tailored to exhibit and study specific features of computation. Typically, a *process* P, specified by some syntax, may non-deterministically execute several *labelled transitions* of the form $P \xrightarrow{a} P'$, where a is an observable effect and P' is a new process. In quantitative process algebras, transitions are labelled by pairs (a,k) where k is a quantity associated to the effect a: thus, $P \xrightarrow{(a,k)} P'$.

We define transition systems where transitions are labelled with symbols from a finite alphabet and from a semiring $\mathbb{K}$. The semantics of a GPA process P is *Multi Labelled Transition System* (*MLTS*) [10]:

Definition 2.5 (MLTS). *A (finite) Multi Labelled Transition System (MLTS) is a five-tuple $MLTS = (S, Act, \mathbb{K}, T, s_0)$, where S is the countable (finite) state space, $s_0 \in S$ is the initial state,*[3] *Act is a finite set of transition labels, $\mathbb{K}$ is a semiring used for the definition of transition costs, and $T : (S \times Act \times S) \longrightarrow \mathbb{K}$ is the transition function.*

Definition 2.6 (GPA syntax [10]). *The set $\mathscr{P}$ of* agents*, or processes, in GPA over a countable set of transition labels Act and a semiring $\mathbb{K}$ is defined by the grammar*

$$P ::= 0 \mid (a,k).P \mid P+P \mid P \|_A P \mid P \backslash A \mid P/A \mid X \mid X \triangleq P$$

where $a \in Act$, $A \subseteq Act \backslash \{\tau\}$ is a subset of actions on which processes synchronise their behaviour, $k \in K$ (the set of values in a semiring $\mathbb{K}$), and X belongs to a countable set of process variables*, coming from a system of co-recursive equations of the form $X \triangleq P$, meaning that X behaves like P. $GPA(\mathbb{K})$ denotes the set of GPA processes labelled with weights in $\mathbb{K}$.*

The formal operational semantics of GPA operators is given in Tab. 1, Informally, process 0 describes inaction or termination; $(a,k).P$ performs a with *value* k and evolves into P; $P+P'$ non deterministically behaves as either P or P'; $P \|_A P'$ describes the process in which P and P' proceed concurrently when they perform actions belonging to A, and independently on all the other actions; $P \backslash A$ expresses the fact that actions from the set A are hidden, i.e., they become τ actions that are no longer usable in joint actions with an environment; the dual, i.e., P/A, restricts the behaviour of P by allowing it to perform only actions not in L.

Given a GPA process P, the set of *derivatives* of a P is defined as $Der(P) = \{P' \mid P \rightarrow^* P'\}$ where $\rightarrow^*$ is $\cup_{a \in Act, k \in K} \xrightarrow{a,k}$; $Sort(P)$ denotes the set of actions names that syntactically appear in P regardless their values.

[3] We simplify the original definition of MLTS given in [10], where an *initialization* function is taken into account to assign a quantitative valuation to each of the n initial states (here we only have one s_0).

$\frac{}{(a,k).P \overset{a,k}{\rightarrow} P}$	$\frac{P \xrightarrow{(a,k)} P_1 \quad P' \xrightarrow{(a,l)} P'_1}{P \Vert_A P' \xrightarrow{(a,k\times l)} P_1 \Vert_A P'_1}\ a \in A$	$\frac{P \xrightarrow{(a,k)} P_1}{X \xrightarrow{(a,k)} P_1} X \triangleq P$
$\frac{P \xrightarrow{(a,k)} P_1}{P \Vert_A, P' \xrightarrow{(a,k)} P_1 \Vert_A P'}\ a \notin A$	$\frac{P_j \xrightarrow{(a,k)} P_1}{\sum_{i\in I} P_i \xrightarrow{(a,k_\Sigma)} P_1}\ j \in I$	$\frac{P' \xrightarrow{(a,k)} P'_1}{P \Vert_A P' \xrightarrow{(a,k)} P \Vert_A P'_1}\ a \notin A$
$\frac{P' \xrightarrow{(a,k)} P'_1}{P\backslash A \xrightarrow{(a,k)} P'_1\backslash A}\ a \notin L$	$\frac{P \xrightarrow{(a_1,k_1)} P' \ldots P \xrightarrow{(a_n,k_n)} P'}{P\backslash A \xrightarrow{(\tau,k_\tau)} P'\backslash A}\ \{a_1,\ldots a_n\} \subseteq A \cup \{\tau\}$	$\frac{P' \xrightarrow{(a,k)} P'_1}{P/A \xrightarrow{(a,k)} P'_1/A}\ a \notin A$

Table 1: An operational semantics for *GPA* [10], where $k_\Sigma = \sum_{i\in I}(P_i \overset{a}{\rightarrow} P_1)$ and $k_\tau = \sum_{i=1}^{n}(k_i)$.

Being $a_1,\ldots,a_n \in Act$, a *trace* is a sequence $(a_1,k_1)\cdots(a_n,k_n)$ leading from process P to process Q. We call $\mathscr{T}(P)$ the set of traces rooted in P. Given a trace $(a_1,k_1)\cdots(a_n,k_n)$, we define its *label* $l(t) = a_1\cdots a_n$, and its *weak run-weight* $|t| = k_1 \times \ldots \times k_n \in K$ (where $\times$ comes from a semiring $\mathbb{K}$). We also define the *strong run-weight* $\|t\|$ of a trace, as the weak-run weight without the weights of τ actions.

Hence, it is possible to *evaluate* the whole behaviour of a process. The valuation of the 0 process is equal to $\top$. We consider processes different form 0 as evaluated in the *optimistic* way, i.e., their evaluation coincides with the value of their best trace(s). Formally, given a process $P \neq 0$, the *weak evaluation-value* is computed as

$$[\![P]\!] = \sum_{\{t\in\mathscr{T}(P)\}}^{\mathbb{K}} |t|,$$

where $\sum^{\mathbb{K}}$ is the set-wise version of the $+$ operator in $\mathbb{K}$. The *strong evaluation-value* is computed as

$$[\![\![P]\!]\!] = \sum_{\{t\in\mathscr{T}(P)\}}^{\mathbb{K}} \|t\|.$$

3 Quantitative Generalized Non Deducibility on Composition

The GNDC schema is a uniform approach for defining several security properties based on the compositionality nature of the process algebra formalism. It has been introduced in [17] to express security properties in a qualitative way. Hereafter, we extend that definition in order to express, in a uniform way, quantitative security properties. Therefore, what we achieve is to be able to quantitatively compare the behaviour of two GPA processes, according to possible different definitions of quantitative behavioural relations (*e.g.*, a weighted trace-equivalence relation).

Hence, we have a quantitative version of the GNDC schema, hereafter denoted as QGNDC, given in terms of GPA:

$$P \in QGNDC_{\triangleleft}^{\alpha,\mathbb{K}} \text{ iff } \forall E \in \mathscr{E}_H : (P\|_H X)\backslash H \triangleleft_{\mathbb{K}} \alpha(P) \tag{1}$$

where $H \subseteq Act\backslash\{\tau\}$ is the set of environmental actions, $\mathscr{E}_H$ is the set of environments, $\triangleleft_{\mathbb{K}} \in \mathscr{P}\times\mathscr{P}$ is a relation between two processes, whose definition depends on the partial order of the semiring $\mathbb{K}$ according to which the processes are quantified and evaluated, and $\alpha : \mathscr{P} \rightarrow \mathscr{P}$ is a function between processes. The $|_H$ is the synchronisation operator stating that all actions in H are performed by the system if and only if both P and E perform them, and the $\backslash H$ is the hiding operator that hides all actions in H. Informally, the $GNDC^{\alpha,\mathbb{K}}_{\triangleleft}$ property requires that the behaviour of process P, once it is composed with any possible environment $E \in \mathscr{E}_H$, is *compliant* with the system expected-behaviour, described by the function α. The notion of compliance depends on the $\triangleleft_{\mathbb{K}}$ relation we select for comparing the behaviours of $(P\|_H X)\backslash H$ and $\alpha(P)$, according not only to an observational equivalence (as in the qualitative approach [17]), but also with respect to order induced by the semiring $\mathbb{K}$.

In the following we provide several definitions of quantitative behavioural-equivalence according to which we are able to specify weighted properties through the QGNDC schema [17]. Furthermore, we compare the expressive power of the different equivalence-relations we define.

3.1 Quantitative Trace-equivalences

One of the basic notions used in the literature to compare processes behaviour is the notion of *trace*: two processes are equivalent if they exactly show the same execution sequences, ands their evaluation scores are comparable in the semiring partial-order. In order to formally define traces, we need a transition relation that does not consider internal moves, denoted by τ. We start by highlighting such τ-actions in execution traces:

Definition 3.1 (weighted weak-trace)**.** *The notation $P \overset{(a,k)}{\Longrightarrow} P'$ is a shorthand for $P \xrightarrow{(\tau,k_\tau)}{}^{*} P_\tau \xrightarrow{(a,k)} P'_\tau \xrightarrow{(\tau,k'_\tau)}{}^{*} P'$, where a (possibly empty) sequence of τ labeled transitions is denoted by $\xrightarrow{(\tau,k_\tau)}{}^{*}$. A* weighted weak-trace *$\gamma = (a_1,k_1)\dots(a_n,k_n) \in (Act\backslash\{\tau\})^*$ is such that $P \overset{\gamma}{\Longrightarrow} P'$ if and only if there exist $P_1,\dots,P_{n-1} \in GPA$ such that $P \overset{(a_1,k_1)}{\Longrightarrow} P_1 \dots P_{n-1} \overset{(a_n,k_n)}{\Longrightarrow} P'$.*

We can now define an equivalence relation based on trace similarity, i.e., the *weak-trace equivalence* ($\approx_{wtrace}$) in Def. 3.2. We require both the strong evaluation-score and the weak evaluation-score of two processes to be equal, or not comparable:

Definition 3.2 (weak-trace equivalence)**.** *For any $P \in \mathscr{P}$ the set $\hat{\mathscr{T}}(P)$ of* weighted weak-traces associated with *P is $\hat{\mathscr{T}}(P) = \{\gamma \in (Act\backslash\{\tau\})^* \mid \exists P' : P \overset{\gamma}{\Longrightarrow} P'\}$, where $(Act\backslash\{\tau\})^*$ is the set of sequences of actions. P and Q are* weak-trace equivalent *(notation $P \approx_{wtrace} Q$) if and only if all the following three conditions hold:*

1. *$\hat{\mathscr{T}}(P) = \hat{\mathscr{T}}(Q)$,*
2. *$[\![\![P]\!]\!] \not\lessgtr_{\mathbb{K}} [\![\![Q]\!]\!]$,[4] and*
3. *$[\![P]\!] \not\lessgtr_{\mathbb{K}} [\![Q]\!]$.*

In the following, we provide an approximate version of weak-trace equivalence, i.e., the *ε-trace relation*. With respect to Def. 3.2, we allow the weak evaluation-score of two processes to differ up to a threshold-value $\varepsilon \in K$.

Definition 3.3 (ε-trace equivalence)**.** *For any $P \in \mathscr{P}$ the set $\hat{\mathscr{T}}(P)$ of* weighted weak-traces associated with *P is $\hat{\mathscr{T}}(P) = \{\gamma \in (Act\backslash\{\tau\})^* \mid \exists P' : P \overset{\gamma}{\Longrightarrow} P'\}$, where $(Act\backslash\{\tau\})^*$ is the set of sequences of actions. P and Q are* ε-trace equivalent *(notation $P \approx_{\varepsilon-trace} Q$) if and only if there exists a value ε such that all the following three conditions hold:*

1. *$\hat{\mathscr{T}}(P) = \hat{\mathscr{T}}(Q)$,*
2. *$[\![\![P]\!]\!] \not\lessgtr_{\mathbb{K}} [\![Q]\!]$, and*

[4] In the following we will use $\not\lessgtr_{\mathbb{K}}$ as a shortcut to denote when two semiring values are equal or not comparable in the poset.

3. $[\![P]\!] \div \varepsilon \geq_{\mathbb{K}} [\![Q]\!] \wedge [\![Q]\!] \div \varepsilon \geq_{\mathbb{K}} [\![P]\!]$.

These relations are comparable one to another. In particular, the following proposition holds.

Proposition 3.1. *For each couple of processes $P, Q \in GPA$. The following statement holds*

$$\forall \varepsilon \in K, \quad P \approx_{wtrace} Q \Rightarrow P \approx_{\varepsilon-trace} Q$$

Note that when $\varepsilon = \top$ we have $P \approx_{wtrace} Q \Leftrightarrow P \approx_{\varepsilon-trace} Q$.

Example 3.1. *Consider two processes $P = (\tau, 1).(a, 3).(b, 2)$ and $Q = (a, 2).(b, 3)$ in the tropical semiring. We have that $P \approx_{1-trace} Q$ (i.e., $\varepsilon = 1$), while $P \approx_{wtrace} Q$ does not hold.*

Note that P and Q in Ex. 3.1 are qualitatively trace-equivalent according to the classic definition given in [17]. Therefore, by considering the weight of traces (i.e., weak-trace equivalence) we obtain a more restrictive equivalence-relation. Consequently, we have introduced the notion ε-trace equivalence with the purpose to gradually be able to relax it and include more processes in the relation.

3.2 Quantitative Bisimulation Equivalences

In this section we focus on the weak-bisimulation equivalence for GPA [10, 27], since we would like to consider as equivalent the behaviour of two processes regardless the weight of internal action τ they perform. Differently from [10], where only the definition of strong bisimulation is provided, we assume that each state of a MLTS has a finite number of transitions with a non-$\top$ weight. In the following, for $\mathscr{R}$ a relation, we write $P\mathscr{R}Q$ to say that $(P, Q) \in \mathscr{R}$.

We extend the definition of quantitative weak bisimulation in [27] by considering a poset of preference values:

Definition 3.4 (quantitative weak-bisimulation)**.** *An equivalence relation $\mathscr{R}$ on $\mathscr{P} \times \mathscr{P}$ is a* quantitative weak bisimulation *if and only if for all $(P, Q) \in \mathscr{R}$ and all $a \in Act$ and each equivalence class $C \in \mathscr{R}$ we have:*

$$\sum_{D \in C} (P \xRightarrow{(a,k)} D) \not\lessgtr \sum_{D \in C} (Q \xRightarrow{(a,k')} D), \qquad \sum_{D \in C} (P \xrightarrow{(\tau,k_\tau)}{}^{*} D) \not\lessgtr \sum_{D \in C} (Q \xrightarrow{(\tau,k'_\tau)}{}^{*} D)$$

We write $P \approx_{\mathbb{K}} Q$ whenever there is a bisimulation $\mathscr{R}$ such that $(P, Q) \in \mathscr{R}$.

Note that the quantitative weak-bisimulation relation holds even if the two values related to P and Q are incomparable in the partial order defined by $+$. In [27] they have to exactly correspond to the same value, since partial orders are not considered.

As accomplished in Sec. 3.1, we define a variant that approximates Def. 3.4, named as *weak ε-bisimulation*. The intuition behind it, similarly to Sec. 3.1, is to relax the cost of τ actions by a threshold-value ε with the purpose to allow two processes to be bismilar (or, better, ε-bisimilar) despite this difference. More precisely, such ε value bounds the difference between the cost of τ actions before and after an action at the same time (see Ex. 3.2).

Definition 3.5 (weak ε-bisimulation)**.** *An equivalence relation $\mathscr{R}$ on $\mathscr{P} \times \mathscr{P}$ is a* weak ε-bisimulation *if and only if, there exists a value ε such that for all $(P, Q) \in \mathscr{R}$ and all $a \in Act$ and each equivalence class $C \in \mathscr{R}$ we have:*

$$\sum_{D \in C} (P \xRightarrow{(a,k)} D) \div \varepsilon \quad \geq_{\mathbb{K}} \quad \sum_{D \in C} (Q \xrightarrow{(a,k')} D) \quad \wedge \quad \sum_{D \in C} (Q \xRightarrow{(a,k)} D) \div \varepsilon \quad \geq_{\mathbb{K}} \quad \sum_{D \in C} (P \xrightarrow{(a,k')} D)$$

$$\sum_{D \in C} (P \xrightarrow{\tau,k_\tau}{}^{*} D) \div \varepsilon \quad \geq_{\mathbb{K}} \quad \sum_{D \in C} (Q \xrightarrow{\tau,k'_\tau}{}^{*} D) \quad \wedge \quad \sum_{D \in C} (Q \xrightarrow{\tau,k_\tau}{}^{*} D) \div \varepsilon \quad \geq_{\mathbb{K}} \quad \sum_{D \in C} (P \xrightarrow{\tau,k'_\tau}{}^{*} D)$$

We write $P \approx_{\varepsilon} Q$ whenever there is a bisimulation $\mathscr{R}$ such that $(P, Q) \in \mathscr{R}$.

These relations are comparable as follows.

Proposition 3.2. *For each couple of processes $P,Q \in GPA$. The following statement holds*

$$\forall \varepsilon \in K \quad P \approx_{\mathbb{K}} Q \Rightarrow P \approx_{\varepsilon} Q$$

Note that when $\varepsilon = \top$ we have $P \approx_{\mathbb{K}} Q \Leftrightarrow P \approx_{\varepsilon} Q$

Example 3.2. *Consider two processes $P = (\tau,3).(a,4).(\tau,5)$ and $Q = (\tau,2).(a,4).(\tau,1)(\tau,1)$ in the tropical semiring. We have that $P \approx_1 Q$ (i.e., $\varepsilon = 1$) while $P \approx_{\mathbb{K}} Q$ does not hold. Instead, if we have two processes $W = (\tau,3).(a,4).(\tau,3)$ and $Y = (\tau,2).(a,4).(\tau,1).(\tau,1)$, $W \approx_2 Y$ (i.e., $\varepsilon = 2$) while $W \approx_1 Y$ does not hold.*

Note that both P and Q, and W and Y in Ex. 3.2 are weak bisimilar according to the classic definition given in [28]. Therefore, by considering the bisimulation relation in Def. 3.4 we obtain a more restrictive equivalence-relation.

4 C-semiring H-M Logic

In the previous section, we have shown how quantitative security properties can be specified by using different quantitative process-equivalences in order to compare the behaviour of a system with respect to the expected one. A different approach for specifying quantitative security-requirements is to express them as a logic formula that the system has to satisfy. It can be useful, for instance, when it is not decidable if two processes are quantitatively equivalent (as defined in Sec. 3). Furthermore, some properties as, for example, *safety properties*[5], can be easily expressed through a logic formula and allow for not requiring the behaviour of the whole system to be checked [15, 24].

For this reason, in the rest of this section we propose a different approach with respect to the one described in Sec. 3, with the purpose to advance an alternative methodology to quantitatively specify the security of a system. Such approach is based on Model Checking and a satisfiability procedure, instead of behavioural equivalences and a comparison checking.

Hence, in order to specify whether a system is secure or not, we need to require that it satisfies a logic formula expressing the intended security-requirements. To this aim, next we propose a quantitative variant of the Hennessy-Milner logic, named c-HM, in such a way to be able to specify a quantitative formula. In particular, differently from [23], where weights are associated to system states, in our approach values are part of transition labels (together with an action): again we consider a MLTS (see Def. 2.5), and we evaluate the satisfaction of a c-HM formula over processes expressed in GPA. In Def. 4.1, we syntactically define the set Φ_M of correct formulas given an MLTS M.

Definition 4.1 (syntax)**.** *Given a MLTS $M = \langle S, Act, \mathbb{K}, T, s_0 \rangle$, and let $a \in Act$, a formula $\phi \in \Phi_M$ is syntactically expressed as follows, where $k \in K$:*

$$\phi ::= k \mid \phi_1 + \phi_2 \mid \phi_1 \times \phi_2 \mid \phi_1 \sqcap \phi_2 \mid \langle a \rangle \phi \mid [a]\phi$$

Clearly we can express more than just true (corresponding to $\top \in K$) and false ($\bot \in K$) through all the values $k \in K$. Semiring operators $+$ (the lub $\sqcup$), glb $\sqcap$, and $\times$ are used in place of classical logic operators $\vee$ and $\wedge$, in order to compose the truth values of two formulas together. As a reminder, when the $\times$ operator is idempotent, then $\times$ and $\sqcap$ coincide (see Sec. 2). Finally, we have the two classical modal operators, i.e., “possibly” ($\langle \cdot \rangle$), and “necessarily” ($[\cdot]$).

[5] E.g., properties expressing that, if something goes wrong, it can be detected in a finite number of steps

$$
\begin{aligned}
&[\![k]\!](s) && = k \in K \;\; \forall s \in S \\
&[\![\phi_1 + \phi_2]\!](s) && = [\![\phi_1]\!](s) + [\![\phi_2]\!](s) \\
&[\![\phi_1 \times \phi_2]\!](s) && = [\![\phi_1]\!](s) \times [\![\phi_2]\!](s) \\
&[\![\phi_1 \sqcap \phi_2]\!](s) && = [\![\phi_1]\!](s) \sqcap [\![\phi_2]\!](s) \\
\\
&[\![\langle a \rangle \phi]\!](s) && = \sum_R (T(s,a,s') \times [\![\phi]\!](s')) \\
\\
&[\![[a]\phi]\!](s) && = \prod_R (T(s,a,s') \times [\![\phi]\!](s')) \\
\\
& && \text{where } R = \{s' \in S \mid s \xrightarrow{a} s' \in T\}
\end{aligned}
$$

Table 2: Semantics of c-HM. $\sum(\emptyset) = \bot$ and $\prod(\emptyset) = \top$.

It is also possible to have a negation operator $\neg : K \longrightarrow K$, which is a unary operator such that, being $A \subseteq Act$, $\neg a \in A$ and $\neg\neg(a) = a$ for all $a \in A$, and $\neg \bigsqcup\{A'\} = \{\neg a \mid a \in A\}$ for all $A' \subseteq A$, where $\bigsqcup$ and $\bigsqcap$ are the set-wise lub and glb operators of the lattice $\langle A, \leq_K \rangle$. The negation operator allows us to use the equivalence $\neg\bot = \top$. Note that the duality $\neg(a+b) = (\neg a) \times (\neg b)$ holds exactly when $\times$ is idempotent. Some examples where negation can be defined are the logical c-semiring, where logical negation is a negation operator, and probabilistic and fuzzy c-semirings, where $1-$ is a negation operator. On the other hand, it is not possible to define a negation operator for the tropical semiring. Hence, the syntax given in Def. 4.1 is proposed without considering the negation operator; otherwise, we can simplify it by removing $\bot$ and $[\,]\phi$, since they can be respectively rewritten as $\neg\top$ and $\neg\langle\,\rangle\neg\phi$.

The semantics of a formula ϕ is given on a particular MLTS $M = \langle S, Act, \mathbb{K}, T, s_0 \rangle$, with the purpose to check the specification defined by ϕ over the behaviour of a weighted transition-system (in Sec. 4.1, M defines the behaviour of a GPA process). Note that, while in [2] the semantics of a formula computes the states $U \subseteq S$ that satisfy that formula, our semantics $[\![\,]\!]_M : (\Phi_M \times S) \longrightarrow K$ (see Tab. 2) computes a truth value (in K) for the same U. For instance, if we use the boolean semiring we always obtain $\top$ iff $U \neq \emptyset$, and $\bot$ otherwise. It is not difficult to extend our semantics to also return U, as in [2]; however, in this work we are focused on computing a degree of satisfaction for ϕ (and U).

In Tab. 2 and in the following (when clear from the context) we omit M from $[\![\,]\!]_M$ for the sake of readability. The semantics is parametrised over a state $s \in S$, which is used to consider only the transitions that can be fired at a given step (labelled with an action a). The first s will be the single initial state of the MLTS we define in Def. 2.5, i.e., s_0.[6]

4.1 Interpreting c-HM over GPA

Both GPA and c-HM logic formulas can be interpreted on a MLTS. In this section, we focus on the interpretation of a c-HM formula ϕ on a GPA process P to provide a notion of *quantitative satisfiability* for the specification described by ϕ, on the behaviour of a process P. First of all, we define the projection of a process on an MLTS.

Definition 4.2 (MLTS projection)**.** *Given an MLTS $M = \langle S, Act, \mathbb{K}, T, s_0 \rangle$, its projection over a process*

[6] Note that is also possible to let the semantics in Tab. 2 be parametrised on a set of states, by aggregating values on all the transitions originating from all of them. For instance, in case we have multiple initial states, as in [10].

P defined over the same M is defined as $M \Downarrow_P = \langle S_P, Act, \mathbb{K}, T_P, s_0 \rangle$, where $S_P = \{s \in S \mid s \in Der(P)\}$ and $T_P = \{(s,a,s') \in S \times Act \times S \mid s, s' \in S_P \wedge a \in Sort(P)\}$.[7]

We are now ready to rephrase the notion of satisfiability to take into account a threshold k (k-satisfiability):

Definition 4.3 ($\models_k$)**.** *A process P satisfies a c-HM formula ϕ with a threshold-value t, i.e., $P \models_t \phi$, if and only if the interpretation of ϕ on $M \Downarrow_P$ is not worse than t. Formally:*

$$P \models_t \phi \Leftrightarrow t \leq [\![\phi]\!]_{M \Downarrow_P}(s_0)$$

This means that P is a model for a formula ϕ (with respect to a certain value t) iff the evaluation of ϕ on P is not worse than t in the partial order defined by $+$ in $\mathbb{K}$. It is worth noting that the interpretation of ϕ on P is independent by the valuation of P itself.

Remark 1. Note that, if P does not satisfy a formula ϕ then $[\![\phi]\!]_{M \Downarrow_P} = \bot$. Consequently, the only t such that $P \models_t \phi$ is $t = \bot$. If $[\![\phi]\!]_{M \Downarrow_P} \neq \bot$, then ϕ is satisfiable with a certain threshold $t \neq \bot$.

Example 4.1. *In order to exemplify the concept expressed here, let us consider a formula ϕ stating that* before opening a document "file2" you have to close an already opened document "file1" . *This is a security property aiming at preserving the confidentiality and integrity of the two documents. ϕ can be expressed by a c-HM formula as follows:*

$$\phi = [\texttt{open\_file1}]([\texttt{close\_file1}][\texttt{open\_file2}]\top \times [\texttt{open\_file2}]\bot)$$

The sub-formula after $\times$ (i.e., $[\texttt{open\_file2}]$) is weighted with $\bot$ because the opening of file2 has to be prevented in case file1 is not closed. Vice-versa, the left-side of $\times$ expresses the right behaviour, and thus it is weighted with $\top$.

Then consider three different processes P and Q, defined on $\langle \mathbb{N}^+ \cup \{+\infty\}, min, \hat{+}, +\infty, 0 \rangle$ (i.e., the tropical semiring):

$$\begin{array}{rcl} P & = & (\texttt{open\_file1}, 5).(\texttt{close\_file1}, 4).0 \\ Q & = & (\texttt{open\_file1}, 3).(\texttt{close\_file1}, 10).0 \\ V & = & (\texttt{open\_file1}, 4).(\texttt{open\_file2}, 2).0 \end{array}$$

According to our definition, $P \models_{11} \phi$ because, referring to Tab. 2, at the first step we consider the cost of the action $\texttt{open\_file1}$, i.e., 5, which is arithmetically summed to

$$[\![([\texttt{close\_file1}][\texttt{open\_file2}]0 \hat{+} [\texttt{open\_file2}]\infty)]\!]_{P'}$$

where $P' = (\texttt{close\_file1}, 4).0$. After $\texttt{close\_file1}$, the process halts, thus $[\![[\texttt{open\_file2}]\infty]\!] = 0$. Finally, we have $[\![\phi]\!]_P = 5 \hat{+} 4 \hat{+} 0 = 9$, which satisfies the asked threshold 11. Q is evaluated in the same way, but since $[\![\phi]\!]_Q = 3 \hat{+} 10 \hat{+} 0 = 13$, we have that $P \not\models_{11} \phi$ because $11 \not\leq 14$. Therefore, even if there is a subset of Q states that satisfies ϕ, the degree satisfaction does not respect the requested threshold. Finally, ϕ is not satisfied by V because $[\![\phi]\!]_V = 5 \hat{+}$ $[\![([\texttt{close\_file1}][\texttt{open\_file2}]0 \hat{+} [\texttt{open\_file2}]\infty)]\!]_{V'} = 4 \hat{+} 2 \hat{+} \infty = \infty$.

5 Quantitative Partial Model Checking

In this section we present a quantitative version of PMC [2], named QPMC, with respect to the parallel composition of GPA processes. Such a function is defined in Tab. 3. Being the logic closed, the interpretation of a formula obtained through the application of such function is straightforward. In Th. 5.1 we report a result similar (i.e., weighted) to the one in [2].

[7] All the processes in parallel share the same s_0.

$$
\begin{array}{lcl}
k_{//_P} & = & k \\
(\phi_1 \times \phi_2)_{//_P} & = & (\phi_1)_{//_P} \times (\phi_2)_{//_P} \\
(\phi_1 + \phi_2)_{//_P} & = & (\phi_1)_{//_P} + (\phi_2)_{//_P} \\
(\phi_1 \sqcap \phi_2)_{//_P} & = & (\phi_1)_{//_P} \sqcap (\phi_2)_{//_P} \\
([a]\phi_1)_{//_P} & = & \begin{cases} [a](\phi_1)_{//_P} \sqcap \displaystyle\bigsqcap_{P \overset{a,k_a}{\rightarrow} P'} ((k_a) \times (\phi_1)_{//_{P'}}) & a \notin L \\ \displaystyle\bigsqcap_{P \overset{a,k_a}{\rightarrow} P'} ((k_a) \times [a](\phi_1)_{//_{P'}}) & a \in L \end{cases} \\
(\langle a \rangle \phi_1)_{//_P} & = & \begin{cases} \langle a \rangle (\phi_1)_{//_P} + \displaystyle\sum_{P \overset{a,k_a}{\rightarrow} P'} ((k_a) \times (\phi_1)_{//_{P'}}) & a \notin L \\ \displaystyle\sum_{P \overset{a,k_a}{\rightarrow} P'} ((k_a) \times \langle a \rangle (\phi_1)_{//_{P'}}) & a \in L \end{cases}
\end{array}
$$

Table 3: A QPMC function.

Theorem 5.1. *Given any two processes P and Q in parallel, and any c-HM formula ϕ, then we have that*

$$[\![\phi]\!]_{P\|_L Q} = [\![\phi_{//_P}]\!]_Q.$$

Sketch[8]. The proposition is proved by induction on the complexity of a formula ϕ.

Base case, $\underline{\phi = \mathbf{k}}$: According to Tab. 2, $[\![k]\!]_{P\|Q} = k = k_{//_P} = [\![k_{//_P}]\!]_Q$.

Inductive Step: As an example, let us now consider two different formulas:

$\underline{\phi = \phi_1 \times \phi_2}$**:** According to Tab. 2 we have that $[\![\phi]\!]_{P\|Q} = [\![\phi_1 \times \phi_2]\!]_{P\|Q} = [\![\phi_1]\!]_{P\|Q} \times [\![\phi_2]\!]_{P\|Q}$. By inductive hypothesis, $[\![\phi_1]\!]_{P\|Q} = [\![(\phi_1)_{//_P}]\!]_Q$ and $[\![\phi_2]\!]_{P\|Q} = [\![(\phi_2)_{//_P}]\!]_Q$. Then $[\![\phi_1]\!]_{P\|Q} \times [\![\phi_2]\!]_{P\|Q} = [\![(\phi_1)_{//_P}]\!]_Q \times [\![(\phi_2)_{//_P}]\!]_Q = [\![(\phi_1)_{//_P} \times (\phi_2)_{//_P}]\!]_Q = [\![(\phi_1 \times \phi_2)_{//_P}]\!]_Q$.

The $+$ and the $\sqcap$ operators can be similarly proved.

$\underline{\phi = \langle \mathbf{a} \rangle \phi_1}$**:** According to Tab. 2, we have

$$[\![\phi]\!]_{P\|Q} = [\![\langle a \rangle \phi_1]\!]_{P\|Q} = \sum_{P\|Q \xrightarrow{(a,k_a)} (P\|Q)'} ((k_a) \times [\![\phi_1]\!]_{(P\|Q)'}).$$

Here we only prove one of several possible cases: if $a \notin L$, then

$$[\![\langle a \rangle \phi_1]\!]_{P\|Q} = \sum_{P\|Q \xrightarrow{(a,k_a)} (P\|Q)'} ((k_a) \times [\![\phi_1]\!]_{(P\|Q)'})$$

where $(P\|Q)'$ is equal to $P'\|Q$ if $P \xrightarrow{(a,k_a)} P'$ or to $P\|Q'$ if $Q \xrightarrow{(a,k_a)} Q'$. Hence,

$$\sum_{P\|Q \xrightarrow{(a,k_a)} (P\|Q)'} ((k_a) \times [\![\phi_1]\!]_{(P\|Q)'}) = \sum_{P \xrightarrow{(a,k_a)} P'} ((k_a) \times [\![\phi_1]\!]_{(P'\|Q)}) + \sum_{Q \xrightarrow{(a,k_a)} Q'} ((k_a) \times [\![\phi_1]\!]_{(P\|Q')}).$$

By inductive hypothesis, this is equal to

$$\sum_{P \xrightarrow{(a,k_a)} P'} ((k_a) \times [\![(\phi_1)_{//_{P'}}]\!]_Q) + \sum_{Q \xrightarrow{(a,k_a)} Q'} ((k_a) \times [\![(\phi_1)_{//_P}]\!]_{Q'}).$$

Hence, $[\![\langle a\rangle\phi_1]\!]_{P\|Q} = \sum_{P\xrightarrow{(a,k_a)}P'} ((k_a)\times[\![(\phi_1)_{//_{P'}}]\!]_Q) + [\![\langle a\rangle(\phi_1)_{//_P}]\!]_Q$. On the other hand,

$$\phi_{//_P} = (\langle a\rangle\phi_1)_{//_P} = \langle a\rangle(\phi_1)_{//_P} + \sum_{P\xrightarrow{(a,k_a)}P'} ((k_a)\times(\phi_1)_{//_{P'}})$$

and its semantics evaluation with respect to the process Q is $[\![(\langle a\rangle\phi_1)_{//_P}]\!]_Q =$

$$[\![\langle a\rangle(\phi_1)_{//_P} + \sum_{P\xrightarrow{(a,k_a)}P'} ((k_a)\times(\phi_1)_{//_{P'}})]\!]_Q = [\![\langle a\rangle(\phi_1)_{//_P}]\!]_Q + [\![\sum_{P\xrightarrow{(a,k_a)}P'} ((k_a)\times(\phi_1)_{//_{P'}})]\!]_Q.$$

Hence $[\![(\langle a\rangle\phi_1)_{//_P}]\!]_Q = [\![\langle a\rangle(\phi_1)_{//_P}]\!]_Q + \sum_{P\xrightarrow{(a,k_a)}P'} ((k_a)\times[\![(\phi_1)_{//_{P'}}]\!]_Q)$, and the two evaluations are equal.

□

Example 5.1. *Let us consider, the tropical semiring* $\langle\mathbb{N}^+\cup\{+\infty\}, min, \hat{+}, +\infty, 0\rangle$*, and two actions* `open` *and* `close` *(*$L=\{\mathtt{open}\}$*). In addition, let us consider a formula* $\phi = [\mathtt{open}]\langle\mathtt{close}\rangle\mathbf{1}$ *stating that once a file is opened, then it has to be closed. We omit the name of the file because not significant for our example. Let P and Q be two GPA processes:*

$$P = (\mathtt{open},5).(\mathtt{close},4).0 + (\mathtt{open},6).0$$
$$Q = (\mathtt{open},4).(\mathtt{close},3).0$$

Let us consider the combined process $P\|_L Q$*, where P and Q synchronise one another on actions in L, i.e., on the action* `open`*. It is easy to see that* $P\|_L Q \models_{20} \phi$*. By applying QPMC to* ϕ *with respect to P we obtain:*

$$\begin{aligned}\phi_{//P} &= (5\times[\mathtt{open}](\langle\mathtt{close}\rangle\mathbf{1})_{//P'})\sqcap(6\times[\mathtt{open}]\langle(\mathtt{close}\rangle\mathbf{1})_{//P'})\\ &= (5\times[\mathtt{open}](\langle\mathtt{close}\rangle\mathbf{1}+(4\times 1))\sqcap(6\times[\mathtt{open}](\langle\mathtt{close}\rangle\mathbf{1}+(4\times 1))\end{aligned}$$

where $+ = \min$, $\times\equiv\hat{+}$, *and* $\sqcap\equiv\max$. *The QPMC function helps to understand which formula Q has to satisfy in order to guarantee that the whole system satisfies the initial requirement. In this simple case, we know the behaviour of Q and we can check if it quantitatively satisfies* $\phi_{//P}$*. To do this, we prove that* $[\![\phi]\!]_{P\|_L Q} = [\![\phi_{//P}]\!]_Q$*. We have:*

$$\begin{aligned}[\![\phi]\!]_{P\|_L Q} &= max(9+(min(4,3)), 10+3) = max(12,13) = 13,\\ [\![\phi_{//P}]\!]_Q &= max(5+(4+min(3,5)), 6+(4+min(3,5))) = max(12,13) = 13.\end{aligned}$$

6 Related Work

The aim of this work is to present a semiring-based formal framework where to deal with quantitative specification of security in combined systems. We dedicate the first part of this section to alternative definitions of quantitative bisimulation relations, in some cases even not applied to security (e.g., [27]).

In [27] the authors extend *Weighted Labelled Transition Systems* (WLTS) towards other behavioural equivalences, by considering semirings of weights. The main result of such work is the definition of a general notion of *weak weighted bisimulation*. They show that this relation coincides with the usual weak bisimulation in case of non-deterministic and fully-probabilistic systems. Moreover, it can also be extended towards kinds of LTSs where this notion is currently missing (e.g., stochastic systems). In Def. 3.3 we also relax quantitative weak-bisimulation to weak ε-bisimulation.

In [1] the authors address the problem of providing a quantitative estimation of the confidentiality of a system by measuring its information leakage. In our analysis the most powerful adversary is measured via a notion of approximate process equivalence. In practice, the lack of information leakage is expressed by a successful weak probabilistic bisimulation based check. Whenever such a check fails, approximate relations relax the conditions imposed by the weak probabilistic-bisimulation, in such a way that the level of approximation represents an estimate of the amount of information leakage. Our notion of ε-bisimulation is very close to [1], except that we generalise it by using semiring operators.

Even the approach in [18] bounds the distance between the transitions of two states: if their distance is less equal than a threshold δ, and this holds for all the states of two processes P_1 and P_2, such processes are said to be approximately bisimilar with a δ-precision. The motivations is that, interacting with the physical world, exact relationships are restrictive and not robust.

The literature also proposes works using fuzzy weights (in this work we have the fuzzy semiring): in [11] a notion of behavioural distance is given to measure the behavioural similarity of non-deterministic fuzzy-transition systems. Two systems are at zero distance if and only if they are bisimilar.

Considering the second fragment of the paper, no direct comparison is available for QPMC. Nevertheless, our c-semiring H-M Logic (see Sec. 4) has been inspired by the work in [23]. Some examples of quantitative temporal logic are [14, 3]. In [14] the authors present *QLTL*, a quantitative analogue of *LTL* and presents algorithms for Model Checking it over a quantitative version of Kripke structures and Markov chains. Thus, weights are in the interval of Real numbers $[0,1]$. In [3] the authors combine robustness scores with the satisfaction probability to optimise some control parameters of a stochastic model: the goal is to best maximise robustness of the desired specifications. However, even this approach is focused on Continuous-Time Markov Chains, and not on semiring algebraic-structures.

Non-binary measures of security have been considered for access control systems by Cheng et al. [12]. The level of security should correspond to a fuzzy domain rather than a strict separation between what is secure and what is not. Zhang et al. define with the BARAC model [31] a notion of benefit for each access, with the underlying idea that allowing an access comes with a benefit for the system. The "value" of an access or an action can be for instance calculated using market-based techniques [29].

From a different perspective, Bielova and Massacci propose in [4] a notion of distance among traces, thus expressing that if a trace is not secure, it should be edited to a secure trace close to the non-secure one, thus characterising enforcement strategies by the distance from the original trace they create. In [13], a similar notion of cost has been introduced following some intuitive leads given in [25] in order to move from qualitative to quantitative enforcement. Semirings have been used by Bistarelli et al. in the context of access control [7] and trust systems [5]. Here we use them in the context of enforcement mechanism defined trough process algebra, following the approach by Buchholz and Kemper [10].

7 Conclusion

We have introduced two different formal-frameworks oriented to the specification of quantitative properties on a GPA-process. Both of the frameworks are have a common *trait d'union* consisting in the use of c-semiring structures to represent transition costs. By taking advantage of such costs, we can constrain classical qualitative-relations between two processes, as we do as our first contribute for trace equivalence and weak bisimulation equivalence. In practice we parametrise the weak bisimulation notion given in [1] by allowing for different metrics, and not probability scores only. At the same time we refine the definition of semiring-based bisimulation given in [27], by extending the relation in order to consider ε-close processes. As a second result, we propose a way to express security constraints via a quantitative version of the Hennessy-Milner logic, and a method for specifying the security of a system through a quantitative version of PMC, which allows us to move a process from the parallel computation to a formula ϕ. If the system satisfies a security property with a value k worse than t (a *security threshold*), then the system is not *quantitatively secure*. In this way we can use this threshold to tradeoff security and functionality/performance requirements.

The essence of the paper is to advance the same basic bricks (i.e., GPA and semirings) with the purpose to enhance two different quantitative frameworks (i.e., process equivalences and PMC), which are nevertheless related by the common purpose of (security) property specification. Of course both of the frameworks can be independently (but still interlacedly) developed to offer a complete specification and validation tool on their own, as the following ideas on future work suggest.

In the future we aim to extend both the approaches in different directions. As an ongoing work, we are investigating on the definition of the characteristic formula of a processes, with respect to each bisimulation equivalence definitions we have provided in Sec. 3. In such way, we will be able to compare the effectiveness of the two proposed approaches. Furthermore, we aim to extend both of them in order to not only use them for the specification has but also for the analysis. Indeed, referring to the former approach, we need to investigate on the characterisation of the most powerful attacker in order to compare the system under attack, with respect to the expected behaviour. This can be done only under certain constraints on the considered equivalences. Referring on the latter approach, we need to elaborate a satisfiability procedure for the quantitative logic we have introduced here in order to verify if the system under investigation is secure or not, i.e., it satisfies the security requirement.

Another possible direction we would like to investigate is the identification of comparative strategies based on the (partial or total) ordering of the semiring. In this way we can compare different strategies and finally synthesise the best one (whether it exists). Another direction is the extension of the framework to use more than one measure associated to each action in order to evaluate a process. Such measures can be combined and ordered, *e.g.*, by using the lexicographical ordering, in such a way that controlling strategies can be selected with respect to the optimisation of the trade-off between some of them.

References

[1] A. Aldini & A. Di Pierro (2008): *Estimating the maximum information leakage*. Int. J. Inf. Sec. 7(3), pp. 219–242.

[2] H. R. Andersen (1995): *Partial Model Checking*. In: *LICS '95*, IEEE Computer Society, p. 398.

[3] E. Bartocci, L. Bortolussi, L. Nenzi & G. Sanguinetti (2013): *On the Robustness of Temporal Properties for Stochastic Models*. In: 2nd International Workshop on Hybrid Systems and Biology, EPTCS 125, pp. 3–19.

[4] N. Bielova & F. Massacci (2011): *Predictability of Enforcement*. In: Proceedings of ESSoS 2011, 6542, Springer, pp. 73–86.

[5] S. Bistarelli, S. N. Foley, B. O'Sullivan & F. Santini (2010): *Semiring-based frameworks for trust propagation in small-world networks and coalition formation criteria*. Security and Communication Networks 3(6), pp. 595–610.

[6] S. Bistarelli & F. Gadducci (2006): *Enhancing Constraints Manipulation in Semiring-Based Formalisms*. In: *ECAI*, pp. 63–67.

[7] S. Bistarelli, F. Martinelli & F. Santini (2012): *A semiring-based framework for the deduction/abduction reasoning in access control with weighted credentials*. *CAMWA* 64(4), pp. 447–462.

[8] S. Bistarelli, U. Montanari & F. Rossi (1997): *Semiring-based constraint satisfaction and optimization*. *J. ACM* 44(2), pp. 201–236.

[9] T. S. Blyth & M. F. Janowitz (1972): *Residuation theory*. 102, Pergamon press Oxford.

[10] P. Buchholz & P. Kemper (2001): *Quantifying the Dynamic Behavior of Process Algebras*. In: *Proceedings of PAPM-PROBMIV '01*, Springer-Verlag, pp. 184–199.

[11] Y. Cao, S. X. Sun, H. Wang & G. Chen (2013): *A Behavioral Distance for Fuzzy-Transition Systems*. *IEEE T. Fuzzy Systems* 21(4), pp. 735–747.

[12] P.-C. Cheng, P. Rohatgi, C. Keser, P. A. Karger, G. M. Wagner & A. S. Reninger (2007): *Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control*. In: *Proceedings of the 2007 IEEE S&P*, IEEE Computer Society, pp. 222–230.

[13] P. Drábik, F. Martinelli & C. Morisset (2012): *Cost-Aware Runtime Enforcement of Security Policies*. In: *STM*, LNCS, pp. 1–16.

[14] M. Faella, A. Legay & M. Stoelinga (2008): *Model Checking Quantitative Linear Time Logic*. *ENTCS* 220(3), pp. 61–77.

[15] R. Focardi & R. Gorrieri (2001): *Classification of Security Properties (Part I: Information Flow)*. In: *FOSAD*, *LNCS* 2171, pp. 331–396.

[16] R. Focardi, R. Gorrieri & F. Martinelli (2004): *Classification of Security Properties - Part II: Network Security*. In: *FOSAD*, *LNCS* 2946, pp. 139–185.

[17] R. Focardi & F. Martinelli (1999): *A Uniform Approach for the Definition of Security Properties*. In: *FM'99 - World Congress on Formal Methods in the Development of Computing Systems*, pp. 794–813.

[18] A. Girard & G. J. Pappas (2007): *Approximation Metrics for Discrete and Continuous Systems*. *IEEE Trans. Automat. Contr.* 52(5), pp. 782–798.

[19] J. A. Goguen & J. Meseguer (1982): *Security Policy and Security Models*. In: *Proc. of the 1982 Symposium on Security and Privacy*, IEEE Press, pp. 11–20.

[20] J. Golan (2003): *Semirings and affine equations over them: theory and applications*. Kluwer Academic Pub.

[21] B. Köpf, P. Malacaria & C. Palamidessi (2013): *Quantitative Security Analysis (Dagstuhl Seminar 12481)*. *Dagstuhl Reports* 2(11), pp. 135–154.

[22] G. Lenzini, F. Martinelli, I. Matteucci & S. Gnesi (2008): *A Uniform Approach to Security and Fault-Tolerance Specification and Analysis*. In: *WADS*, pp. 172–201.

[23] A. Lluch-Lafuente & U. Montanari (2005): *Quantitative mu-calculus and CTL defined over constraint semirings*. *TCS* 346(1), pp. 135–160.

[24] F. Martinelli & I. Matteucci (2007): *An Approach for the Specification, Verification and Synthesis of Secure Systems*. *ENTCS* 168, pp. 29–43.

[25] F. Martinelli, I. Matteucci & C. Morisset (2012): *From qualitative to quantitative enforcement of security policy*. In: *Proceedings of MMM-ACNS'12*, Springer-Verlag, pp. 22–35.

[26] Fabio Martinelli, Ilaria Matteucci & Francesco Santini: *Semiring-based Specification Approaches for Quantitative Security*.

[27] M. Miculan & M. Peressotti (2013): *Weak bisimulations for labelled transition systems weighted over semirings*. *CoRR* abs/1310.4106.

[28] R. Milner (1999): *Communicating and mobile systems: the π-calculus*. Cambridge University Press.

[29] I. Molloy, P.-C. Cheng & P. Rohatgi (2008): *Trading in risk: using markets to improve access control*. In: *Workshop on New Security Paradigms*, NSPW '08, ACM, pp. 107–125.

[30] S. Rudeanu & D. Vaida (2004): *Semirings in Operations Research and Computer Science: More Algebra*. *Fundam. Inf.* 61(1), pp. 61–85.

[31] L. Zhang, A. Brodsky & S. Jajodia (2006): *Toward Information Sharing: Benefit And Risk Access Control (BARAC)*. In: *Proceedings of POLICY'06*, IEEE Computer Society, pp. 45–53.