©2012 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. Original IEEE publication: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6169562

Security Requirements for Uniformly Parameterised Cooperations

Peter Ochsenschläger and Roland Rieke
Fraunhofer Institute for Secure Information Technology, SIT
Darmstadt, Germany
Email: peter-ochsenschlaeger@t-online.de, roland.rieke@sit.fraunhofer.de

***Abstract*—The specification of security requirements is an important step when specifying new systems and systems of systems or analysing existing systems with regard to security issues. A common way to formally specify security requirements is by means of safety and liveness properties. The systems in the focus of this paper are uniformly parameterised cooperations. Such systems are characterised by the composition of a set of identical components. These components interact in a uniform manner described by the schedules of the partners. Such a kind of interaction is typical for scalable complex systems with a cloud or grid structure. As a main result, a formalism to specify uniformly parameterised behaviour properties of cooperations is given. To capture possibilistic aspects of especially liveness properties, a modified satisfaction relation is used. For safety properties, this relation, which is called approximate satisfaction, is equivalent to the usual one.**

***Keywords*-security requirements specification; safety properties; possibilistic liveness properties; approximate satisfaction; uniformly parameterised behaviour properties**

I. Introduction

The systems in the focus of this paper are *uniformly parameterised cooperations*. Such systems are characterised by (i) the composition of a set of identical components (copies of a two-sided cooperation); and (ii) the fact that these components "interact" in a uniform manner (described by the schedules of the partners). Such a kind of interaction is typical for scalable complex systems. As an example of such uniformly parameterised systems of cooperations, e-commerce protocols can be considered. In these protocols, the two cooperation partners have to perform a certain kind of financial transactions. Such a protocol should work for several partners in the same manner, and the mechanism (schedule) to determine how one partner may be involved in several cooperations is the same for each partner. So, the cooperation is parameterised by the partners and the parameterisation should be uniform w.r.t. the partners.

To model the functional requirements of dependable systems, satisfying to high degrees both fault-tolerance and security attributes, three distinct classes of (system specification) properties; namely *safety*, *liveness* and *information flow*, are of interest [1]. Security requirements for such systems can be formalised by safety and liveness properties. A formal definition of safety and liveness properties is proposed in [2]. In [3] we defined a satisfaction relation, called *approximate satisfaction*, which expresses a possibilistic view on liveness and is equivalent to the satisfaction relation in [2] for safety properties.

Safety properties typically cover the aspects of authenticity, integrity, non-repudiation and authorisation requirements, e.g., to prevent man-in-the-middle attacks and attacks based on violation of access rights. Liveness properties cover availability aspects, such as denial of service attacks or attacks forcing a system into a state where only a reduced functionality is possible. Furthermore, liveness properties are often used to express desirable features of a system like correct termination, occurrence, responsiveness, and precedence [4].

As a main result of the work presented, a framework for *uniformly parameterised behaviour properties* of cooperations is given. A modified satisfaction relation is used to capture possibilistic aspects of especially liveness properties. The proofs of the theorems and the usual formal notations are given in [5].

II. Parameterised Cooperations

To describe a two-sided cooperation, let $\Sigma = \Phi \cup \Gamma$ where Φ is the set of actions of cooperation partner F and Γ is the set of actions of cooperation partner G and $\Phi \cap \Gamma = \emptyset$. Now a prefix closed language $L \subset (\Phi \cup \Gamma)^*$ formally defines a two-sided cooperation. For parameter sets I, K and $(i,k) \in I \times K$ let Σ_{ik} denote pairwise disjoint copies of Σ. The elements of Σ_{ik} are denoted by a_{ik} and $\Sigma_{IK} := \bigcup_{(i,k)\in I\times K} \Sigma_{ik}$. The index ik describes the bijection $a \leftrightarrow a_{ik}$ for $a \in \Sigma$ and $a_{ik} \in \Sigma_{ik}$. Now $\mathscr{L}_{IK} \subset \Sigma_{IK}^*$ (prefix-closed) describes a *parameterised system*. To avoid pathological cases we generally assume parameter and index sets to be non empty.

For $(i,k) \in I \times K$, let $\pi_{ik}^{IK} : \Sigma_{IK}^* \to \Sigma^*$ with

$$\pi_{ik}^{IK}(a_{rs}) = \begin{cases} a \mid & a_{rs} \in \Sigma_{ik} \\ \varepsilon \mid & a_{rs} \in \Sigma_{IK} \setminus \Sigma_{ik} \end{cases} .$$

For *uniformly parameterised systems* $\mathscr{L}_{IK}$ we generally want to have

$$\mathscr{L}_{IK} \subset \bigcap_{(i,k)\in I\times K} ((\pi_{ik}^{IK})^{-1}(L))$$

because from an abstracting point of view, where only the actions of a specific Σ_{ik} are considered, the complex system $\mathscr{L}_{IK}$ is restricted by L.

In addition to this inclusion $\mathscr{L}_{IK}$ is defined by *local schedules* that determine how each "version of a partner" can participate in "different cooperations". More precisely, let $SF \subset \Phi^*$, $SG \subset \Gamma^*$ be prefix closed. For $(i,k) \in I \times K$, let $\varphi_i^{IK} : \Sigma_{IK}^* \to \Phi^*$ and $\gamma_k^{IK} : \Sigma_{IK}^* \to \Gamma^*$ with

$$\varphi_i^{IK}(a_{rs}) = \begin{cases} a \mid & a_{rs} \in \Phi_{\{i\}K} \\ \varepsilon \mid & a_{rs} \in \Sigma_{IK} \setminus \Phi_{\{i\}K} \end{cases} \text{ and}$$

$$\gamma_k^{IK}(a_{rs}) = \begin{cases} a \mid & a_{rs} \in \Gamma_{I\{k\}} \\ \varepsilon \mid & a_{rs} \in \Sigma_{IK} \setminus \Gamma_{I\{k\}} \end{cases},$$

where Φ_{IK} and Γ_{IK} are defined correspondingly to Σ_{IK}.

Definition 1 (uniformly parameterised cooperation)**.** *Let I, K be finite parameter sets, then*

$$\mathscr{L}_{IK} := \bigcap_{(i,k)\in I\times K} (\pi_{ik}^{IK})^{-1}(L) \cap \bigcap_{i\in I} (\varphi_i^{IK})^{-1}(SF) \cap \bigcap_{k\in K} (\gamma_k^{IK})^{-1}(SG)$$

denotes a uniformly parameterised cooperation*.*

By this definition

$$\mathscr{L}_{\{1\}\{1\}} = (\pi_{11}^{\{1\}\{1\}})^{-1}(L) \cap (\varphi_1^{\{1\}\{1\}})^{-1}(SF) \cap (\gamma_1^{\{1\}\{1\}})^{-1}(SG).$$

As we want $\mathscr{L}_{\{1\}\{1\}}$ being isomorphic to L by the isomorphism

$$\pi_{11}^{\{1\}\{1\}} : \Sigma_{\{1\}\{1\}}^* \to \Sigma^*$$

we additionally need

$$(\pi_{11}^{\{1\}\{1\}})^{-1}(L) \subset (\varphi_1^{\{1\}\{1\}})^{-1}(SF) \text{ and}$$
$$(\pi_{11}^{\{1\}\{1\}})^{-1}(L) \subset (\gamma_1^{\{1\}\{1\}})^{-1}(SG).$$

This is equivalent to $\pi_\Phi(L) \subset SF$ and $\pi_\Gamma(L) \subset SG$, where $\pi_\Phi : \Sigma^* \to \Phi^*$ and $\pi_\Gamma : \Sigma^* \to \Gamma^*$ are defined by

$$\pi_\Phi(a) = \begin{cases} a \mid & a \in \Phi \\ \varepsilon \mid & a \in \Gamma \end{cases} \text{ and } \pi_\Gamma(a) = \begin{cases} a \mid & a \in \Gamma \\ \varepsilon \mid & a \in \Phi \end{cases}.$$

So we complete Def. 1 by the additional conditions

$$\pi_\Phi(L) \subset SF \text{ and } \pi_\Gamma(L) \subset SG.$$

The system $\mathscr{L}_{IK}$ of cooperations is a typical example of a *complex system*. It consists of several identical components (copies of the two-sided cooperation L), which "interact" in a uniform manner (described by the schedules SF and SG and by the homomorphisms φ_i^{IK} and γ_k^{IK}).

Remark 1. *It is easy to see that $\mathscr{L}_{IK}$ is isomorphic to $\mathscr{L}_{I'K'}$ if I is isomorphic to I' and K is isomorphic to K'. More precisely, let $\iota_{I'}^{I} : I \to I'$ and $\iota_{K'}^{K} : K \to K'$ be bijections and let $\iota_{I'K'}^{IK} : \Sigma_{IK}^* \to \Sigma_{I'K'}^*$ be defined by*

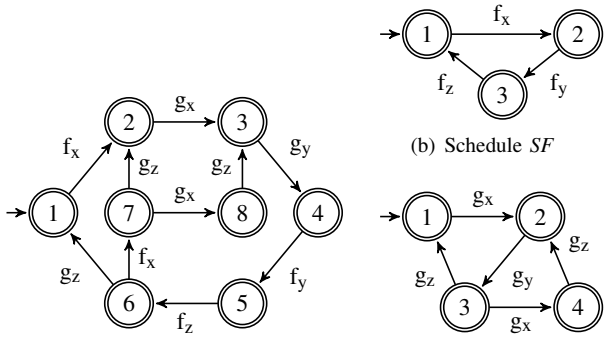
$$\iota_{I'K'}^{IK}(a_{ik}) := a_{\iota_{I'}^{I}(i)\iota_{K'}^{K}(k)} \text{ for } a_{ik} \in \Sigma_{IK}.$$

Then $\iota_{I'K'}^{IK}$ is a isomorphism and $\iota_{I'K'}^{IK}(\mathscr{L}_{IK}) = \mathscr{L}_{I'K'}$. The set of all these isomorphisms $\iota_{I'K'}^{IK}$ defined by corresponding bijections $\iota_{I'}^{I}$ and $\iota_{K'}^{K}$ is denoted by $\mathscr{I}_{I'K'}^{IK}$.

To illustrate the concepts of this paper, we consider the following example, which was introduced in [6].

Example 1. *We consider a system of servers, each of them managing a resource, and clients, which want to use these resources. We assume that as a means to enforce a given* privacy policy *a server has to manage its resource in such a way that no client may access this resource during it is in use by another client (*privacy requirement*). This may be required to ensure* anonymity *in such a way that clients and their actions on a resource cannot be linked by an observer.*

We formalise this system at an abstract level, where a client may perform the actions $\mathrm{f_x}$ (send a request), $\mathrm{f_y}$ (receive a permission) and $\mathrm{f_z}$ (send a free-message), and a server may perform the corresponding actions $\mathrm{g_x}$ (receive a request), $\mathrm{g_y}$ (send a permission) and $\mathrm{g_z}$ (receive a free-message). So $\Phi = \{\mathrm{f_x}, \mathrm{f_y}, \mathrm{f_z}\}$ and $\Gamma = \{\mathrm{g_x}, \mathrm{g_y}, \mathrm{g_z}\}$ and hence $\Sigma = \{\mathrm{f_x}, \mathrm{f_y}, \mathrm{f_z}, \mathrm{g_x}, \mathrm{g_y}, \mathrm{g_z}\}$. The possible sequences of actions of a client resp. of a server are given by the automaton $\mathbb{SF}$ resp. $\mathbb{SG}$. The automaton $\mathbb{L}$ describes the 1-1-cooperation of one client and one server (see Fig. 1). These automata define the client-server system $\mathscr{L}_{IK}$. Incoming arrows denote initial states and double circles denote final states. In $\mathbb{L}$ all states are final states, since L is prefix closed.



(a) 1-1-cooperation L (b) Schedule SF (c) Schedule SG

Figure 1. Automata $\mathbb{L}$, $\mathbb{SF}$ and $\mathbb{SG}$ for Example 1

By *self-similarity* [6] we formalise that for $I' \subset I$ and $K' \subset K$ from an abstracting point of view, where only the actions of $\Sigma_{I'K'}$ are considered, the complex system $\mathscr{L}_{IK}$ behaves like the smaller subsystem $\mathscr{L}_{I'K'}$. Therefore we now consider special abstractions on $\mathscr{L}_{IK}$.

Definition 2 (projection abstraction)**.** *For $I' \subset I$ and $K' \subset K$ let $\Pi_{I'K'}^{IK} : \Sigma_{IK}^* \to \Sigma_{I'K'}^*$ with*

$$\Pi_{I'K'}^{IK}(a_{rs}) = \begin{cases} a_{rs} \mid & a_{rs} \in \Sigma_{I'K'} \\ \varepsilon \mid & a_{rs} \in \Sigma_{IK} \setminus \Sigma_{I'K'}. \end{cases}$$

Definition 3 (self-similarity)**.** *A uniformly parameterised cooperation $\mathscr{L}_{IK}$ is called* self-similar *iff*

$$\Pi^{IK}_{I'K'}(\mathscr{L}_{IK}) = \mathscr{L}_{I'K'} \text{ for each } I' \times K' \subset I \times K.$$

Self-similarity is a generalisation of $\pi^{IK}_{ik}(\mathscr{L}_{IK}) = L$.
In [5] we show that example 1 is self-similar.

III. Uniformly Parameterised Behaviour Properties

Behaviour properties E of systems are intersections of safety and liveness properties [2]. Intuitively a safety property stipulates that "something bad does not happen" and a liveness property stipulates that "something good eventually happens". In [2] both classes, as well as system behaviour, are formalised in terms of ω-languages.

Definition 4 (linear satisfaction)**.** *According to [2], a property E of a system is a subset of Σ^ω. If $S \subset \Sigma^\omega$ represents the behaviour of a system, then S* linearly satisfies *E iff $S \subset E$.*

Safety properties $E_s \subset \Sigma^\omega$ are of the form $E_s = \Sigma^\omega \setminus F\Sigma^\omega$ with $F \subset \Sigma^*$, where F is the set of "bad things".

Liveness properties $E_l \subset \Sigma^\omega$ are characterised by $\text{pre}(E_l) = \Sigma^*$. A typical example of a liveness property is

$$E_l = (\Sigma^* M)^\omega \text{ with } \emptyset \neq M \subset \Sigma^+. \quad (1)$$

This E_l formalises that "always eventually a finite action sequence $m \in M$ happens".

We describe system behaviour by prefix closed languages $B \subset \Sigma^*$. So, in order to apply the framework of [2], we have to "transform" B into an ω-language. This can be done by the *limit* $\lim(B)$. For prefix closed languages $B \subset \Sigma^*$, their limit is defined by

$$\lim(B) := \{w \in \Sigma^\omega | \text{pre}(w) \subset B\}.$$

If B contains maximal words u (deadlocks), then these u are not "captured" by $\lim(B)$. Formally the set $\max(B)$ of all maximal words of B is defined by

$$\max(B) := \{u \in B | \text{ if } v \in B \text{ with } u \in \text{pre}(v), \text{ then } v = u\}.$$

Now, using a dummy action #, B can be unambiguously described by

$$\hat{B} := B \cup \max(B)\#^* \subset \hat{\Sigma}^*,$$

where $\# \notin \Sigma$ and $\hat{\Sigma} := \Sigma \cup \{\#\}$. By this definition, in $\hat{B}$ the maximal words of B are continued by arbitrary many #'s. So $\hat{B}$ does not contain maximal words.

By this construction, we now can assume that system behaviour is formalised by prefix closed languages $\hat{B} \subset \Sigma^*\#^* \subset \hat{\Sigma}^*$ without maximal words, and the corresponding infinite system behaviour $S \subset \Sigma^\omega$ is given by $S := \lim(\hat{B})$.

For such an S and safety properties

$$E_s = \hat{\Sigma}^\omega \setminus F\hat{\Sigma}^\omega \text{ with } F \subset \hat{\Sigma}^*$$

it holds

$$S \subset E_s \text{ iff } S \cap F\hat{\Sigma}^\omega = \emptyset \text{ iff } \text{pre}(S) \cap F = \emptyset \text{ iff } \hat{B} \cap F = \emptyset. \quad (2)$$

If $F \subset \Sigma^*$ then $\hat{B} \cap F = \emptyset$ iff $B \cap F = \emptyset$. So

$$S \subset E_s \text{ iff } B \cap F = \emptyset \text{ for } F \subset \Sigma^*. \quad (3)$$

Let $h : \Sigma^* \to \Sigma'^*$ be an alphabetic homomorphism and $F' \subset \Sigma'^*$, then $h(L) \cap F' = \emptyset$ iff $L \cap h^{-1}(F') = \emptyset$. As $h^{-1}(F') \subset \Sigma^*$, (3) implies

$$\lim(\hat{B}) \subset \hat{\Sigma}^\omega \setminus h^{-1}(F')\hat{\Sigma}^\omega \text{ iff } \lim(\widehat{h(B)}) \subset \hat{\Sigma}'^\omega \setminus F'\hat{\Sigma}'^\omega. \quad (4)$$

So by (3) and (4) our approach in [6] is equivalent to the ω-notation of safety properties described by $F \subset \Sigma^*$, and the relation $S \subset E_s$, is compatible with abstractions with respect to such safety properties. Linear satisfaction is too strong for systems in our focus with respect to liveness properties, because $S = \lim(\hat{L})$ can contain "unfair" infinite behaviours, which are not elements of E_l. Let for example $I \supset \{1,2\}$ and $K \supset \{1\}$ then $\lim(\widehat{\mathscr{L}_{IK}}) \cap \Sigma^\omega_{\{1\}\{1\}} \neq \emptyset$ (infinite action sequences, where only the partners with index 1 cooperate). If $E_l = \Sigma^*_{IK}\Sigma_{\{2\}\{1\}}\Sigma^\omega_{IK}$ then $\lim(\widehat{\mathscr{L}_{IK}}) \not\subset E_l$.

Instead of neglecting such unfair infinite behaviours, we use a weaker satisfaction relation, called *approximate satisfaction*, which implicitly expresses some kind of fairness.

Definition 5 (approximate satisfaction)**.** *A system $S \subset \hat{\Sigma}^\omega$* approximately satisfies *a property $E \subset \hat{\Sigma}^\omega$ iff each finite behaviour (finite prefix of an element of S) can be continued to an infinite behaviour, which belongs to E. More formally, $pre(S) \subset pre(S \cap E)$.*

In [3] it is shown, that for safety properties

linear and approximate satisfaction are equivalent. (5)

With respect to approximate satisfaction, liveness properties stipulate that "something good eventually is possible".

Concerning properties E not of the form $E = \hat{\Sigma}^\omega \setminus F\hat{\Sigma}^\omega$ with $F \subset \Sigma^*$ approximate satisfaction is not compatible with abstractions in such sense, that there exist pairs of concrete and abstract systems related by homomorphisms such that the abstract system approximately satisfies such a property E but the concrete system does not approximately satisfy a "corresponding" property. In [3] such examples are discussed and a property of abstractions is given that overcomes this problem. This property is called *simplicity* of an alphabetic homomorphism $h : \Sigma^* \to \Sigma'^*$ with respect to a prefix closed language $B \subset \Sigma^*$ and it is formalised in terms of continuation possibilities in B and $h(B)$.

Definition 6. *An alphabetic language homomorphism $h : \Sigma^* \to \Sigma'^*$ is* simple *on $B \subset \Sigma^*$ iff for each $w \in B$ there exists $u \in h(w)^{-1}(h(B))$ such that $u^{-1}(h(w^{-1})(B))) = u^{-1}(h(w)^{-1}(h(B)))$.*

There are several sufficient conditions for simplicity. For our purpose the following is helpful.

Theorem 1. *If for each $y \in B$ there exists $z \in y^{-1}(B)$ with $h((yz)^{-1}(B)) = (h(yz))^{-1}(h(B))$ then h is simple on B.*

To formulate the implication of simplicity we have to "extend" h to $\hat{\Sigma}^\omega$. Let $\hat{h} : \hat{\Sigma}^* \to \widehat{\Sigma'}^*$ be the homomorphisms defined by $\hat{h}(a) := h(a)$ for $a \in \Sigma$ and $\hat{h}(\#) := \#$.

$$\begin{aligned} &\text{For } x \in \hat{\Sigma}^\omega \text{ either } \lim(\hat{h}(\mathrm{pre}(x))) = \{y\} \subset \widehat{\Sigma'}^\omega \\ &\text{or } \max(\hat{h}(\mathrm{pre}(x))) = \{z\} \subset \Sigma'^*. \end{aligned} \tag{6}$$

Now let $\hat{h}_\omega : \hat{\Sigma}^\omega \to \widehat{\Sigma'}^\omega$ be defined for $x \in \hat{\Sigma}^\omega$ by $\hat{h}_\omega(x) := y$ if $\lim(\hat{h}(\mathrm{pre}(x))) = \{y\} \subset \widehat{\Sigma'}^\omega$ and $\hat{h}_\omega(x) := z\{\#\}^\omega$ if $\max(\hat{h}(\mathrm{pre}(x))) = \{z\} \subset \Sigma'^*$. $\hat{h}_\omega$ is not an homomorphism but it has the following properties:
If $w = uv \in \hat{\Sigma}^\omega$ with $u \in \hat{\Sigma}^*$ and $v \in \hat{\Sigma}^\omega$ then

$$\hat{h}_\omega = \hat{h}(u)\hat{h}_\omega(v). \tag{7}$$

If $w' = u'a'v' \in \widehat{\Sigma'}^\omega$ with $u' \in \widehat{\Sigma'}^*$, $a' \in \Sigma'$, $v' \in \widehat{\Sigma'}^\omega$ and $w \in \hat{\Sigma}^\omega$ with $\hat{h}_\omega(w) = w'$ then

$$\begin{aligned} &w = uav \text{ with } u \in \hat{\Sigma}^*, a \in \Sigma, v \in \hat{\Sigma}^\omega, \\ &\hat{h}(u) = u', h(a) = a' \text{ and } \hat{h}_\omega(v) = v'. \end{aligned} \tag{8}$$

In [3] the following has been proven:

Theorem 2. *If h is simple on a regular prefix closed language B then*

$$\begin{aligned} &pre(lim(\widehat{h(B)})) \subset pre(lim(\widehat{h(B)}) \cap E') \text{ implies} \\ &pre(lim(\hat{B})) \subset pre(lim(\hat{B}) \cap \hat{h}_\omega^{-1}(E')) \end{aligned}$$

for each $E' \subset \widehat{\Sigma'}^\omega$.

Here $\hat{h}_\omega^{-1}(E')$, which is approximately satisfied by the concrete system $\lim(\hat{B})$, is the corresponding property to E', which is approximately satisfied by the abstract system $\lim(\widehat{h(B)})$. It has been proven that simplicity of h on B is necessary for the set of implications in theorem 2.

In [6] safety properties are formalised by formal languages $F \subset \Sigma^*$ and it is defined that a prefix closed language $B \subset \Sigma^*$ satisfies such a safety property F iff $L \cap F = \emptyset$. By (3) and (5) this is equivalent to the statement that $\lim(\hat{L})$ approximately satisfies the safety property

$$\hat{\Sigma}^\omega \setminus F\hat{\Sigma}^\omega. \tag{9}$$

In [6] uniformly parameterised safety properties are generated by safety properties $\mathring{F} \subset \Sigma^*_{\mathring{I}\mathring{K}}$. They are defined in such a way that a parameterised system $\mathscr{L}_{IK} \subset \Sigma^*_{IK}$ satisfies the generated parameterised safety property iff $\mathscr{L}_{IK}$ satisfies each safety property $(\Pi^{IK}_{I'K'})^{-1}(\iota^{\mathring{I}\mathring{K}}_{I'K'}(\mathring{F}))$ with $I' \subset I$, $K' \subset K$ and $\iota^{\mathring{I}\mathring{K}}_{I'K'} \in \mathscr{I}^{\mathring{I}\mathring{K}}_{I'K'}$, where $\mathscr{I}^{\mathring{I}\mathring{K}}_{I'K'}$ is the set of all isomorphisms $\iota^{\mathring{I}\mathring{K}}_{I'K'} : \Sigma^*_{\mathring{I}\mathring{K}} \to \Sigma^*_{I'K'}$ generated by bijections $\iota^{\mathring{I}}_{I'} : \mathring{I} \to I'$ and $\iota^{\mathring{K}}_{K'} : \mathring{K} \to K'$ in such a way that

$$\iota^{\mathring{I}\mathring{K}}_{I'K'}(a_{ik}) := a_{\iota^{\mathring{I}}_{I'}(i)\iota^{\mathring{K}}_{K'}(k)} \tag{10}$$

for $a_{ik} \in \Sigma_{\mathring{I}\mathring{K}}$. We now want to generalise this idea to arbitrary system properties formulated as subsets of $\hat{\Sigma}^\omega$. For index sets $\mathring{I}$, I', $\mathring{K}$ and K' each bijection $\iota^{\mathring{I}}_{I'} : \mathring{I} \to I'$ and $\iota^{\mathring{K}}_{K'} : \mathring{K} \to K'$ generates an isomorphism $\hat{\iota}^{\mathring{I}\mathring{K}}_{I'K'} : \hat{\Sigma}^*_{\mathring{I}\mathring{K}} \to \hat{\Sigma}^*_{I'K'}$ by $\hat{\iota}^{\mathring{I}\mathring{K}}_{I'K'}(a) := \iota^{\mathring{I}\mathring{K}}_{I'K'}(a)$ for $a \in \Sigma_{\mathring{I}\mathring{K}}$ and $\hat{\iota}^{\mathring{I}\mathring{K}}_{I'K'}(\#) := \#$. For each $w \in \hat{\Sigma}^\omega_{\mathring{I}\mathring{K}}$ $\lim(\hat{\iota}^{\mathring{I}\mathring{K}}_{I'K'}(\mathrm{pre}(w))) = \{w'\} \in \hat{\Sigma}^\omega_{I'K'}$. Now the mapping $\widehat{\iota\omega}^{\mathring{I}\mathring{K}}_{I'K'} : \hat{\Sigma}^\omega_{\mathring{I}\mathring{K}} \to \hat{\Sigma}^\omega_{I'K'}$ defined for each $w \in \hat{\Sigma}^\omega_{\mathring{I}\mathring{K}}$ by

$$\widehat{\iota\omega}^{\mathring{I}\mathring{K}}_{I'K'}(w) := w' \text{ with } \lim(\hat{\iota}^{\mathring{I}\mathring{K}}_{I'K'}(\mathrm{pre}(w))) = \{w'\},$$

is a bijection. The set of all these bijections $\widehat{\iota\omega}^{\mathring{I}\mathring{K}}_{I'K'}$ we denote by $\widehat{\mathscr{I}\omega}^{\mathring{I}\mathring{K}}_{I'K'}$. $\widehat{\iota\omega}^{\mathring{I}\mathring{K}}_{I'K'}$ is "like an isomorphism" because for each $w \in \hat{\Sigma}^\omega_{\mathring{I}\mathring{K}}$ holds:

$$\begin{aligned} &w = uv \text{ with } u \in \hat{\Sigma}^*_{\mathring{I}\mathring{K}} \text{ and } v \in \hat{\Sigma}^\omega_{\mathring{I}\mathring{K}} \\ &\text{iff } \widehat{\iota\omega}^{\mathring{I}\mathring{K}}_{I'K'}(w) = \hat{\iota}^{\mathring{I}\mathring{K}}_{I'K'}(u)\widehat{\iota\omega}^{\mathring{I}\mathring{K}}_{I'K'}(v). \end{aligned} \tag{11}$$

For finite index sets $\mathring{I}$, I, $\mathring{K}$ and K let

$$\hat{\mathscr{I}}[(\mathring{I},\mathring{K}),(I,K)] := \bigcup_{I' \subset I, K' \subset K} \widehat{\mathscr{I}\omega}^{\mathring{I}\mathring{K}}_{I'K'}.$$

Note that

$$\hat{\mathscr{I}}[(\mathring{I},\mathring{K}),(I,K)] = \emptyset \text{ if } |\mathring{I}| > |I| \text{ or } |\mathring{K}| > |K|, \tag{12}$$

where $|I|$ denotes the cardinality of the set I.

Now let $\mathring{E} \subset \widehat{\Sigma_{\mathring{I}\mathring{K}}}^\omega$, with fixed index sets $\mathring{I}$ and $\mathring{K}$, be an arbitrary property. Motivated by theorem 2 and [6] for finite index sets I and K we define

$$\mathscr{E}^{\mathring{E}}_{IK} := [((\widehat{\Pi^{IK}_{I'K'}})_\omega)^{-1}(\widehat{\iota\omega}^{\mathring{I}\mathring{K}}_{I'K'}(\mathring{E}))]_{\widehat{\iota\omega}^{\mathring{I}\mathring{K}}_{I'K'} \in \hat{\mathscr{I}}[(\mathring{I},\mathring{K}),(I,K)]}. \tag{13}$$

We say that

$$\begin{aligned} &\lim(\widehat{\mathscr{L}_{IK}}) \textit{ approximately satisfies such a family } \mathscr{E}^{\mathring{E}}_{IK} \\ &\textit{of properties} \text{ iff} \\ &\lim(\widehat{\mathscr{L}_{IK}}) \text{ approximately satisfies each of the properties} \\ &((\widehat{\Pi^{IK}_{I'K'}})_\omega)^{-1}(\widehat{\iota\omega}^{\mathring{I}\mathring{K}}_{I'K'}(\mathring{E})) \text{ for } \widehat{\iota\omega}^{\mathring{I}\mathring{K}}_{I'K'} \in \hat{\mathscr{I}}[(\mathring{I},\mathring{K}),(I,K)]. \end{aligned} \tag{14}$$

On account of (12) it makes sense to consider finite families of $\mathscr{E}^{\mathring{E}}_{IK}$.

Definition 7 (uniformly parameterised behaviour property)**.** *Let T, I and K be finite index sets. For each $t \in T$ let $\mathring{E}_t \subset \widehat{\Sigma_{\mathring{I}_t\mathring{K}_t}}^\omega$ and $\mathscr{E}^{\mathring{E}_t}_{IK}$ be defined as in* (13)*. Then $\mathscr{E}_{IK} := (\mathscr{E}^{\mathring{E}_t}_{IK})_{t \in T}$ is called a* uniformly parameterised behaviour property.

We say that $lim(\widehat{\mathscr{L}_{IK}})$ approximately satisfies *$\mathscr{E}_{IK}$ iff $lim(\widehat{\mathscr{L}_{IK}})$ approximately satisfies each $\mathscr{E}^{\mathring{E}_t}_{IK}$ for $t \in T$ as defined in* (14)*.*

If $\mathring{E} = \widehat{\Sigma_{\mathring{I}\mathring{K}}}^\omega \setminus \mathring{F}\widehat{\Sigma_{\mathring{I}\mathring{K}}}^\omega$ with $\mathring{F} \subset \Sigma^*_{\mathring{I}\mathring{K}}$ then by (11)

$$\widehat{\iota\omega}^{\mathring{I}\mathring{K}}_{I'K'}(\mathring{E}) = \widehat{\Sigma_{I'K'}}^\omega \setminus \iota^{\mathring{I}\mathring{K}}_{I'K'}(\mathring{F})\widehat{\Sigma_{I'K'}}^\omega$$

and by (7) and (8)

$$((\widehat{\Pi^{IK}_{I'K'}})_\omega)^{-1}(\widehat{\iota\omega}^{\mathring{I}\mathring{K}}_{I'K'}(\mathring{E})) = \widehat{\Sigma_{IK}}^{\omega} \setminus (\Pi^{IK}_{I'K'})^{-1}(\iota^{\mathring{I}\mathring{K}}_{I'K'}(\mathring{F}))\widehat{\Sigma_{IK}}^{\omega}.$$

Now (9) and (10) imply that definition 7 generalises the corresponding definitions of [6]. If $\Pi^{IK}_{I'K'}$ is simple on a regular $\mathscr{L}_{IK}$ for $I' \subset I$ and $K' \subset K$ and if $\mathring{E} \subset \widehat{\Sigma_{\mathring{I}\mathring{K}}}^{\omega}$ is an arbitrary property, then by theorem 2 $\lim(\widehat{\mathscr{L}_{IK}})$ approximately satisfies $((\widehat{\Pi^{IK}_{I'K'}})_\omega)^{-1}(\widehat{\iota\omega}^{\mathring{I}\mathring{K}}_{I'K'}(\mathring{E}))$ if $\lim(\widehat{\Pi^{IK}_{I'K'}(\mathscr{L}_{IK})})$ approximately satisfies $\widehat{\iota\omega}^{\mathring{I}\mathring{K}}_{I'K'}(\mathring{E})$. If $\mathscr{L}_{IK}$ is self-similar, then $\Pi^{IK}_{I'K'}(\mathscr{L}_{IK}) = \mathscr{L}_{I'K'}$ for each $I' \subset I$ and $K' \subset K$. If $\widehat{\iota\omega}^{\mathring{I}\mathring{K}}_{I'K'} \in \widehat{\mathscr{I}\omega}^{\mathring{I}\mathring{K}}_{I'K'}$ then by (11) $\lim(\widehat{\mathscr{L}_{I'K'}})$ approximately satisfies $\widehat{\iota\omega}^{\mathring{I}\mathring{K}}_{I'K'}(\mathring{E})$ iff $\lim(\widehat{\mathscr{L}_{\mathring{I}\mathring{K}}})$ approximately satisfies $\mathring{E}$. So we get

Theorem 3. *Let I, K, $\mathring{I}$ and $\mathring{K}$ be finite index sets with $|\mathring{I}| \leq |I|$ and $|\mathring{K}| \leq |K|$. Let $\mathscr{L}_{IK}$ be a uniformly parameterised, self-similar regular system of cooperations and let $\Pi^{IK}_{I'K'}$ simple on $\mathscr{L}_{IK}$ for each $I' \subset I$ and $K' \subset K$ with $|\mathring{I}| = |I'|$ and $|\mathring{K}| = |K'|$. Then for $\mathring{E} \subset \widehat{\Sigma_{\mathring{I}\mathring{K}}}^{\omega}$ $\lim(\widehat{\mathscr{L}_{IK}})$ approximately satisfies $\mathscr{E}^{\mathring{E}}_{IK}$ if $\lim(\widehat{\mathscr{L}_{\mathring{I}\mathring{K}}})$ approximately satisfies $\mathring{E}$.*

Many practical liveness properties are of the form (1). Let us consider a prefix closed language $B \subset \Sigma^*$ and a formal language $\emptyset \neq M \subset \Sigma^+$. By definition 5 $\lim(\hat{B})$ approximately satisfies $(\hat{\Sigma}^* M)^\omega$ iff each $u \in B$ is prefix of $v \in B$ with

$$v^{-1}(B) \cap M \neq \emptyset. \tag{15}$$

If B and M are regular sets, then (15) can be checked by usual automata algorithms without referring to $\lim(\hat{B}) \cap (\hat{\Sigma}^* M)^\omega$. If $h : \Sigma^* \to \Sigma'^*$ is an alphabetic homomorphism and $M' \subset \Sigma^+$, then by (7) and (8)

$$\hat{h}^{-1}_\omega((\hat{\Sigma}'^* M')^\omega) = (\hat{\Sigma}^* h^{-1}(M'))^\omega \subset \hat{\Sigma}^\omega, \tag{16}$$

which is also of the form (1). Let us now consider the prefix closed language $L \subset \Sigma^*$ of example 1 and the "phase" $P \subset \Sigma^+$ given by the automaton $\mathbb{P}$ in Fig. 2.

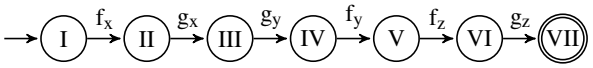


Figure 2. Automaton $\mathbb{P}$

$\lim(\hat{L})$ approximately satisfies the liveness property $(\hat{\Sigma}^* P)^\omega \subset \hat{\Sigma}^*$, because the automaton $\mathbb{L}$ in Fig. 1(a) is strongly connected and $P \subset L$. (17)

(17) states that in the 1-1-cooperation $\lim(\hat{L})$ always eventually a "complete run through the phase P" is possible.

Let now $\mathring{P} := (\pi^{\{1\}\{1\}}_{11})^{-1}P \subset \Sigma^+_{\{1\}\{1\}}$ and $\mathring{E} := (\widehat{\Sigma_{\{1\}\{1\}}}^* \mathring{P})^\omega \subset \widehat{\Sigma_{\{1\}\{1\}}}^{\omega}$. As $\pi^{\{1\}\{1\}}_{11} : \Sigma^*_{\{1\}\{1\}} \to \Sigma^*$ is an isomorphism then by (17) $\lim(\widehat{\mathscr{L}_{\{1\}\{1\}}})$ approximately satisfies $\mathring{E}$.

$\mathscr{L}_{IK}$ is regular in example 1, and in [5] it is shown that $\mathscr{L}_{IK}$ is self-similar. So if we prove simplicity of $\Pi^{IK}_{I'K'}$ on $\mathscr{L}_{IK}$, then by theorem 3

$$\lim(\widehat{\mathscr{L}_{IK}}) \text{ approximately satisfies } \mathscr{E}^{\mathring{E}}_{IK} \tag{18}$$

for each finite indes set I and K. A concept to prove simplicity of $\Pi^{IK}_{I'K'}$ on $\mathscr{L}_{IK}$, based on theorem 1, is subject of a forthcoming paper. By (16) (18) states that for each pair of clients and servers always eventually a "complete run through a phase P" is possible w.r.t. the abstraction, where only the actions of this client and server are considered.

IV. Conclusions and Future Work

In [6] we have shown, in particular, that for self-similar parameterised systems $\mathscr{L}_{IK}$, the parameterised problem of verifying a *uniformly parameterised safety property* can be reduced to finitely many fixed finite state problems.

Extending this, the main result of the present paper is a formal framework for *uniformly parameterised behaviour properties* capturing the full spectrum of safety and liveness. This uniformly parameterisation fits exactly to the scalability and reliability issues of complex systems such as, for example, cloud computing platforms. A combination of these properties can now be used to specify security requirements for such kinds of systems.

Acknowledgement

Roland Rieke developed the work presented here in the context of the project MASSIF (ID 257475) being co-funded by the European Commission within FP7.

References

[1] Z. Benenson, F. C. Freiling, T. Holz, D. Kesdogan, and L. D. Penso, "Safety, liveness, and information flow: Dependability revisited." in *ARCS Workshops*, ser. LNI, W. Karl, J. Becker, K.-E. Gropietsch, C. Hochberger, and E. Maehle, Eds., vol. 81. GI, 2006, pp. 56–65.

[2] B. Alpern and F. B. Schneider, "Defining liveness," *Information Processing Letters*, vol. 21, no. 4, pp. 181–185, October 1985.

[3] U. Nitsche and P. Ochsenschläger, "Approximately satisfied properties of systems and simple language homomorphisms," *Information Processing Letters*, vol. 60, pp. 201–206, 1996.

[4] B. Anderson, J. Hansen, P. Lowry, and S. Summers, "The application of model checking for securing e-commerce transactions," *Communications of the ACM*, vol. 49, no. 6, pp. 97–101, 2006.

[5] P. Ochsenschläger and R. Rieke, "Behaviour Properties of Uniformly Parameterised Cooperations," Fraunhofer SIT, Tech. Rep. SIT-TR-2010/2, 2010. [Online]. Available: http://sit.sit.fraunhofer.de/smv/publications

[6] ——, "Security properties of self-similar uniformly parameterised systems of cooperations," in *Proceedings of the 19th Euromicro International Conference on Parallel, Distributed and Network-Based Computing (PDP)*. IEEE Computer Society, February 2011.