Overview of Approach

1. Uniform parameterisations of cooperations are defined.
   - Each pair of partners cooperates in the same manner.
   - The mechanism (schedule) to determine how one partner may be involved in several cooperations, is the same for each partner.
2. By generalising this, self-similarity is formalised.
3. Uniformly parameterised behaviour properties are defined.
   - safety: something bad does not happen
   - liveness: something good eventually happens
   + fairness: something good eventually is possible
4. The parameterised problem of verifying such a property is reduced by self-similarity and simplicity of the abstraction to a finite state problem.
5. An example for a finite state verification of uniformly parameterised behaviour properties is given (in the paper).
Uniformly Parameterised Cooperations

Prefix closed language $L$ formally defines a two-sided cooperation

Example: Automaton for an iterated handshake of $F$ and $G$

$\mathcal{L}_{IK} \subset \Sigma_{IK}^*$ describes a parameterised cooperation

Example: Automaton for the 1-2-cooperation $\mathcal{L}_{\{1\}}\{1,2\}$

State space explosion problem

Example: Automaton for the 2-1-cooperation $\mathcal{L}_{\{1,2\}}\{1\}$

A 3-3-cooperation with the same simple behaviour of partners already requires an automaton with 916 states and 3168 state transitions.
Each pair of partners cooperate restricted by $L$

For uniformly parameterised systems $L_{IK}$ we generally want to have

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

with

$$\pi_{ik}(a_{rs}) = \left\{ \begin{array}{l}
a \mid a_{rs} \in \Sigma_{ik} \\
\epsilon \mid a_{rs} \in \Sigma_{IK} \setminus \Sigma_{ik}
\end{array} \right..$$

Restriction by local schedule $SG$

Local schedules determine how each "version of a partner" can participate in "different cooperations".

$$L_{IK} \subset \bigcap_{k \in K} (\gamma_{k}^{-1}(SG)),$$

with

$$\gamma_{k}(a_{rs}) = \left\{ \begin{array}{l}
a \mid a_{rs} \in \Gamma_{I(k)} \\
\epsilon \mid a_{rs} \in \Gamma_{IK} \setminus \Gamma_{I(k)}
\end{array} \right..$$

Automaton for the 2-1-cooperation $\mathcal{L}_{\{1,2\}}$

Uniformly Parameterised Cooperation

- Each pair of partners cooperates in the same manner.
- The mechanism (schedule) to determine how one partner may be involved in several cooperations, is the same for each partner.

Definition (uniformly parameterised cooperation $L_{IK}$)

Let $I$, $K$ be finite parameter sets and $\pi_{\Phi}(L) \subset SF$, $\pi_{\Gamma}(L) \subset SG$, then

$$L_{IK} := \bigcap_{(i,k) \in I \times K} (\pi_{ik})^{-1}(L) \cap \bigcap_{i \in I} (\phi_{i}^{-1}(SF)) \cap \bigcap_{k \in K} (\gamma_{k}^{-1}(SG))$$

$\pi_{\Phi}: \Sigma^{*} \rightarrow \Phi^{*}$ and $\pi_{\Gamma}: \Sigma^{*} \rightarrow \Gamma^{*}$ are defined by

$$\pi_{\Phi}(a) = \left\{ \begin{array}{l}
a \mid a \in \Phi \\
\epsilon \mid a \in \Gamma
\end{array} \right.$$

and $\pi_{\Gamma}(a) = \left\{ \begin{array}{l}
a \mid a \in \Gamma \\
\epsilon \mid a \in \Phi
\end{array} \right..$

Remark: $\mathcal{L}_{\{1\}} \subset L$.
Self-similarity

Abstracting point of view
- Only actions of some selected partners \( \Sigma_{IK'} \) are considered.
- The complex system \( \mathcal{L}_{IK} \) of all partners behaves like the smaller subsystem \( \Sigma_{IK'} \) of selected partners.

Definition (Self-similarity)
A uniformly parameterised cooperation \( \mathcal{L}_{IK} \) is self-similar iff
\[
\Pi_{IK'}^{IK} (\mathcal{L}_{IK}) = \mathcal{L}_{IK'} \text{ for each } I' \times K' \subset I \times K,
\]
where \( \Pi_{IK'}^{IK}(a_{rs}) = \{ a_{rs} \mid a_{rs} \in \Sigma_{IK'} \} \) and \( \Pi_{IK'}^{IK}(a_{rs}) = \emptyset \) for \( a_{rs} \notin \Sigma_{IK} \setminus \Sigma_{IK'} \).

System Properties
A property \( E \) of a system is a subset of \( \Sigma^\omega \). If \( S \subset \Sigma^\omega \) represents the behaviour of a system, then \( S \) linearly satisfies \( E \) iff \( S \subset E \).

Alpern/Schneider: Each property \( E \) is the intersection of a safety and a liveness property
Safety properties \( E_s \subset \Sigma^\omega \) are of the form \( E_s = \Sigma^\omega \setminus \bar{F} \Sigma^\omega \) with \( F \subset \Sigma^+ \), where \( F \) is the set of “bad things”.
Liveness properties \( E_l \subset \Sigma^\omega \) are characterised by \( \text{pre}(E_l) = \Sigma^+ \).

Reliability: Typical example of a liveness property
\[
E_l = (\Sigma^+ M)^\omega \text{ with } \emptyset \neq M \subset \Sigma^+.
\] (1)
“always eventually a finite action sequence \( m \in M \) happens”

Counterexample
\[
\Pi_{IK'}^{IK}(\mathcal{L}_{IK}) \not\subset \mathcal{L}_{IK'}
\]

Approximate Satisfaction
Linear satisfaction is too strong w.r.t. to liveness properties, because \( S = \lim (\hat{B}) \) can contain “unfair” infinite behaviours, which are not in \( E \).

If in a 2-1-cooperation infinite action sequences exist where only the partners with index 1 cooperate, i.e., \( \lim (\mathcal{L}_{IK}) \cap \Sigma^\omega \not\subset \emptyset \),
then e.g. \( E = \Sigma^+ \Sigma_{[2]}(1) \Sigma^\omega \) is not linearly satisfied; \( \lim (\mathcal{L}_{IK}) \not\subset E \).

A weaker satisfaction relation implicitly expresses a kind of fairness.

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 \( E \), i.e. \( \text{pre}(S) \subset \text{pre}(S \cap E) \).

With respect to approximate satisfaction, liveness properties stipulate that “something good” eventually is possible.
Property Preserving Abstractions

**Theorem (1)**

Simple homomorphisms define exactly the class of such abstractions, for which holds that each property is approximately satisfied by the abstract behaviour if and only if the “corresponding” property is approximately satisfied by the concrete behaviour of the system.

A system approximately satisfies a property if and only if each finite behaviour can be continued to an infinite behaviour, which satisfies the property.

Combining the introduced Concepts

**Theorem**

Let \( I, K, \hat{I}, \hat{K} \) be finite index sets with \( |\hat{I}| \leq |I| \) and \( |\hat{K}| \leq |K| \).

Let \( \mathcal{L}_{IK} \) be a

- uniformly parameterised,
- self-similar regular system of cooperations, and
- the abstracting view \( \Pi_{IK}^{\hat{K}} \) on actions of selected partners \( I', K' \) be simple on \( \mathcal{L}_{IK} \) for each \( I \subset I', K' \subset K \) with \( |I| = |I'|, |\hat{K}| = |K'| \).

If an abstract system \( \text{lim}(\hat{\mathcal{L}}_{IK}) \)

approximately satisfies a property \( E \subset \hat{\Sigma}_{IK}^\omega \),

then the concrete system \( \text{lim}(\mathcal{L}_{IK}) \)

approximately satisfies the “corresponding” family of properties \( \mathcal{E}_{IK}^E \).

Conclusions

**Previous work**

- The parameterised problem of verifying a uniformly parameterised safety property can be reduced to finitely many finite state problems.

**Main result of the presented work**

- A formal framework for uniformly parameterised behaviour properties capturing the full spectrum of safety and liveness.
- Uniformly parameterisation of behaviour properties fits to the reliability issues of scalable systems, e.g., cloud computing.
- A combination of these properties can now be used to specify security requirements for such kinds of systems.

**Further Work**

- Concept to prove simplicity of \( \Pi^{\hat{K}}_{IK} \) on \( \mathcal{L}_{IK} \)
- Construction principles for uniformly parameterised self-similar systems

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.