Composition and Formal Validation in Reactive Adaptive Middleware

Annie Ressouche — Jean-Yves Tigli — Oscar Carrillo

N° 7541
February 2011
Composition and Formal Validation in Reactive Adaptive Middleware

Annie Ressouche*, Jean-Yves Tigli†, Oscar Carrillo‡

Domain : Perception, Cognition, Interaction
Équipe-Projet Pulsar

Rapport de recherche n° 7541 — February 2011 — 27 pages

Abstract: Nowadays, adaptive middleware plays an important role in the design of applications in ubiquitous and ambient computing. Currently most of these systems manage the adaptation at the middleware intermediary layer. Dynamic adaptive middleware are then decomposed into two levels: a first one to simplify the development of distributed systems using devices, a second one to perform dynamic adaptations within the first level. In this report we consider component-based middleware and a corresponding compositional adaptation. Indeed, the composition often involves conflicts between concurrent adaptations. Thus we study how to maintain consistency of the application in spite of changes of critical components and conflicts that may appear when we compose some component assemblies. Relying on formal methods, we provide a well defined representation of component behaviors. In such a setting, model checking techniques are applied to ensure that concurrent access does not violate expected and acceptable behaviors of critical components.

Key-words: service oriented middleware, event-based composition, reliability, formal methods, synchronous modeling, validation

* Inria Sophia-Antipolis Méditerranée
† I3S Laboratory and CNRS (Rainbow)
‡ Inria Sophia-Antipolis Méditerranée
Composition et vérification formelle dans les middlewares réactifs et adaptatifs

Résumé : De nos jours, les middlewares adaptatifs et réactifs jouent un rôle important dans la conception d’applications dans le domaine de l’informatique ubiquitaire et ambiante. Généralement, ces systèmes réalisent cette adaptation au niveau intermédiaire du middleware. Ainsi, les middlewares adaptatifs sont décomposés en deux parties : une première partie qui permet un développement simplifié des systèmes distribués utilisant des dispositifs, une seconde qui réalise les adaptations dynamiques de la première partie. Dans ce rapport nous considérons des middlewares à base de composants et un adaptation compositionnelle. Mais souvent lors d’une composition certaines adaptations concurrentes s’avèrent conflictuelles. Pour résoudre ce problème, nous étudions comment préserver la consistence d’une application lors de changements concernant certains composants critiques, avec des conflits qui peuvent apparaître quand on compose des assemblages de composants. Nous utilisons des méthodes formelles pour modéliser le comportement des composants afin de bénéficier des techniques de vérification par model checking et ainsi prouver que des accès concurrents respectent les comportements acceptables des composants critiques.

Mots-clés : middleware orientés services, composition par événements, sûreté de fonctionnement, méthodes formelles, modèles synchrones, validation
1 Introduction

Ubiquitous computing follows an evolution of computer science introduced by Weiser [27] two decades ago. A major consequence is the arrival of applications more and more opened on everyday environment relying on objects supposedly communicating and intelligent. Devices managed in ubiquitous computing are nowadays heterogeneous, variable, and interacting with a physical environment. Moreover, applications in this domain must often face some variability during execution time. Moving with a mobile user, such applications have not always access to the same devices. Thus, it turns out that the appearance and disappearance of these latter need a dynamic evolution of the application. Hence, evolving in a real environment, ubiquitous applications must be able to react to changes in the surrounding physical environment.

Then, it is a real challenge to address these constraints for middleware. Indeed, now they must support a stable applicative model in spite of a heterogeneous and variable software infrastructure. Actually, middleware must be
reactive (they must react to context change) and adaptive (they must adapt themselves continuously to context changes).

1.1 Component-based Adaptive and Reactive Middleware

Historically, [22] defines two extremes in the range of strategies for adaptation. At one extreme, adaptation is entirely the responsibility of individual applications. The other extreme of application-transparent adaptation places entire responsibility for adaptation on the system. Currently most of the work converge to manage the adaptation at the middleware intermediary layer [1]. In this last case dynamic adaptive middleware are then decomposed into two levels [8]. The primary level of middleware is to simplify the development of distributed systems [12]. The second level performs dynamic adaptations within middleware.

Because ubiquitous computing is based on preexisting devices, middleware must manage legacy of black-box of software pieces. Three kinds of approaches are well suited to manage such constraints : component oriented middleware, service oriented middleware and more recently new popular approaches using components assembly to compose preexisting services like, SCA or SLCA ([24]).

The second level of adaptive middleware manage dynamic modifications of the first one to perform adaptation. According to [17] we can distinguish two main approaches to implement software adaptation. The first one is parameter adaptation. For component based middleware this approach consists in modifying components variables that determine their behavior. The second one is compositional adaptation. This approach allows component-based middleware to change dynamically components with others in response to changes in its execution environment. In this paper we study how to maintain consistency of the application in spite of critical components changes and conflicts that may appear when we superpose component assemblies in mechanisms for compositional adaptation. Indeed in such cases, we need to use verification techniques to check safety and various other correctness properties of the evolving application.

1.2 Need for Validation

Then, the main motivation appears when we introduce new requirements for ubiquitous applications such as safety. Indeed, few research works in ubiquitous computing address some partly critical applications. For example, many ubiquitous applications address health care domain without validating some critical functionalities. Anyway, safety is an important concern in adaptive middleware. Applications may intervene in critical systems (i.e. system whose failure or malfunction may result in death or serious injury to people, or loss or severe damage to equipment or environmental harm). Components may have to satisfy stringent constraints related to security and should be submitted to formal verification and validation. Moreover, context change adaptation should preserve safety rules. Then key problems are : (1) how to specify and validate the behavior of one assembly connected to a critical component (Cf. section 3), (2) in case of multiple assemblies sharing some critical components, how to compose them and validate properties of the overall application (Cf. section 4).
1.3 Our proposal

Our previous works rely on the advice paradigm (detailed in section 5.1) to compose component assemblies. Different languages have been supplied to apply this paradigm. One of the most efficient allows to compose assemblies verifying the symmetric property of the composition (commutativity, associatively, indempotence for the composition between proposed component assemblies to weave) [4, 23]. Nevertheless such an approach doesn’t allow to define properly how to deal with potential conflict in concurrent multiple access to a component not previously known by the language. For example, concurrent access to a new light component with implicit semantics doesn’t allow managing safely the consequences of the concurrent access to light.on and light.off events. Indeed, for new components, it is interesting to describe an advice as an assembly factory in a user-friendly manner using a language. But this is not sufficient to solve the potential conflicts in concurrent access to unknown new components.

The major contribution of this work is to show that formal methods (and particularly synchronous modelling framework) offer means to automatically validate critical component behaviors and to prove safety property preservation through a sound composition operation useful to perform context adaptation. Thus we extend our component-based adaptive middleware with specific tools to allow validation of local composition on critical devices and services, using model checking techniques.

The report is organized as follows: next section (??) briefly describes the component-based middleware use we consider and introduce the example we rely on all along the report to illustrate our approach. It is extracted from a use case in the domain of health care for elderly. Then section 3 presents our solution which introduces synchronous monitors to model critical devices expected behaviors. They support formal validation. In section 4 we introduce a composition operation between synchronous monitors preserving validated properties. Such an approach allows us to offer a deterministic solution to multiple access to critical devices. We discuss the practical issues of our work in section 5. We introduce our reactive adaptive middleware for ubiquitous computing, named WComp and also its extension with verification facilities. Then we describe the implementation of the example in our middleware. In section 6 we compare our approach with different works which address the problem of reliability of middleware for ubiquitous computing. Finally, section 7 concludes and open the way for future works.

2 Component-based Middleware Use

In this work, we consider middleware where communication means are event-based. Of course event-driven systems are not suitable for very complex design, but adequate for reactivity, dynamicity and high adaptability. In our approach such components are often proxies for services for device and then must reflect the device behavior. Some of them are critical and we want to validate their usage within some middleware assemblies.

We illustrate our approach with the design of (a small part of) an application in the domain of health care for elderly. The purpose is to monitor old adult in an instrumented home, using sensing technology. There are different kinds
of sensors in the environment: video cameras, contact sensors to indicate closed or opened status of equipment, wearable sensors, etc. In this framework, we are deep in the domain where reactive and adaptive middleware solutions apply, since some sensors can appear and disappear (particularly wearable ones). In this example, we show the design of a small part of a project dedicated to observe activities of daily living (ADLs) in an equipped home 1. We consider the recognition of activities related to kitchen usage. The goal is to send several kinds of alarms depending on sensor observation results. Component proxies are associated to four sensors: a contact sensor on the fridge which indicates the state of the door (opened or closed); a timer which sends a minute information; a camera which locates a person; a posture sensor which tells if the person is standing, sitting or lying. This latter is a wearable device composed by accelerometers.

In this application, an Alarm component proxy receives three kinds of alarms: warning, weak, alarm and strong alarm. It is linked with assemblies of components for fridge and timer sensors, camera sensor and posture sensor. This Alarm component is critical and we will ensure that it raises the appropriate alarm in the designed application. To this aim, we offer a mean to ensure that each output event coming from one of the designed assemblies for sensors is correctly sent. Indeed, we supply a new component reflecting the behaviors of (assemblies of) components and we check that these latter are used out of harm’s way (see section 3.1.2). Moreover, it is not sufficient to individually prove that each new component outputs are not misused. We also must ensure that the combination of two output events coming from two different assemblies and linked with the same input event of Alarm component works correctly. Thus we introduce a safe composition between components (see section 4.1).

3 Components with Validated Behaviors

To validation purpose, we introduce models to describe the behavior of application components. Finite automata are well adapted to the representation of device behaviors and moreover provide a lot of verification tools based on efficient model-checking techniques to verify properties.

3.1 Component Behavior Modelling.

3.1.1 Component Behavior as Synchronous Models

The aim is to define means to represent component behavior. These components listen to events coming from other components or from an input environment and will provide output events in reaction. They have to satisfy stringent constraints (correctness, response time) and they should be submitted to formal verification and validation as they may intervene in a critical decision. Thus determinism would be an important advantage. A way of reducing the complexity of behavior description is to consider them evolve through successive phases. During one phase, only the external events which were present at the beginning of the phase and the internal events that occurred as a consequence of the first ones are considered. The phase ends when some stability (fixed-point) has been

1http://gerhome.cstb.fr/
achieved (or when an external clock decides that it is over). We call such a phase an instant. Indeed, during such an instant, time seems to be suspended (the external events are frozen). Such an instant-based representation will be called a synchronous model. In such models, a reaction has no duration because its real duration is delayed to the next clock cycle or next instant of the system.

This issue characterizes the synchronous hypothesis on which all synchronous models rely. A significant way well suited to validation is to express them as Mealy machines [18]. Mealy machines are both finite automata and synchronous models. Indeed a transition in Mealy machines corresponds to a reaction or an instant of the system.

The Mealy machines we consider are 5-uple of the shape: $< Q, q^{init}, I, O, T, \lambda >$, where $Q$ is a finite set of states; $q^{init} \in Q$ is the initial state. $I$ (resp. $O$) is a finite set of input (resp. output) events; $T \subseteq Q \times Q$ is the transition relation. $\lambda$ is a labeling function: $\lambda : T \times I^B \mapsto 2^O \cup \{\epsilon\}$ where $I^B$ is the set of Boolean expressions over $I^2$. It is a Boolean algebra with standard interpretation for $true, false, \cdot, +$ and $\neg$ 3. Finally, $\epsilon$ represents an undefined event 4. In short, $q \xrightarrow{i/o} q'$ will denote a transition with the agreement: $(q,q') \in T$ and $\lambda((q,q'),i) = o$. Furthermore, according to the synchronous hypothesis, we want our model deterministic and reactive:

1. $q \xrightarrow{i/o} q_1$ and $q \xrightarrow{i/o} q_2 \in T \Rightarrow q_1 = q_2$ and $o_1 = o_2$ (determinism)

2. $\forall i \in I^B, \forall q \in Q, \exists q' \xrightarrow{i/o} q' \in T$ (reactivity)

### 3.1.2 Synchronous Monitors

Critical components will provide a synchronous model of their behavior and some additional properties (constraints) checked when component is used. This model is designed as a Mealy machine where each output is connected with an input event of the critical component. Indeed, let us consider a synchronous monitor specified as the Mealy machine $M = < Q, q^{init}, I, O, T, \lambda >$ and connected to a critical component with $I_C$ as input event set. There must exist an injective mapping: $in : O \mapsto I_C$.

Figure 1 illustrates such a situation. It shows a part of the application introduced in section ??.

---

2 Its elements are built according to the following grammar: $e := true | false | I | e \cdot e | e + e | \neg e$.

3 We will consider usual Boolean algebra rules to infer equality between two elements of $I^B$.

4 For short, we will denote $X \cup \{\epsilon\}$ as $X_\epsilon$. 
Composition and Formal Validation in Reactive Adaptive Middleware

Figure 2: The posture monitor is a Mealy machine($\langle Q_3, q_{init}^3, I_3, O_3, T_3, \lambda_3 \rangle$) with an only state and two transitions.

posture sensor and connected to the Alarm component. Thus, we will define a synchronous monitor to describe the behavior of the assembly. This posture monitor listens to $I_3 = \{\text{sitting, standing, lying}\}$ input event set. Its output event set is $O_3 = \{\text{warning}_3, \text{weak\_alarm}_3\}$. It emits a warning$_3$ event when the person is sitting or standing and a weak\_alarm$_3$ event when he/she is lying. This monitor is detailed in figure 2.

Finally, the critical Alarm proxy component has $I_A = \{\text{warning}, \text{weak\_alarm}, \text{strong\_alarm}\}$ as input event set and there is an injection $\text{in} : O_3 \mapsto I_A$: \[
\begin{align*}
in(\text{warning}_3) &= \text{warning} \\
in(\text{weak\_alarm}_3) &= \text{weak\_alarm}
\end{align*}
\]

A synchronous model becomes a monitor component beyond the unsafe proxy component. Then, safety and liveness properties concerning critical component usage can be verified using model-checking tools.

3.2 Component Behavior Validation

Among others validation techniques, the model-checking approach [6, 16] requires a model of systems against which formulas are checked for satisfaction. The model must express all the possible behaviors of the system, the formulas depict required properties of such behaviors. Synchronous Mealy machines are well suited to express these behaviors and they are relevant models to apply model checking techniques.

The properties may be formalized as formulas of a formal logic interpreted over automata. A popular logic is CTL* (computation tree logic see [16]). It contains universal and existential quantification over model paths, as well as temporal operators expressing that a property holds in the next state, or in every state (safety properties), or in some state (liveness properties). Nowadays, a lot of tools [5, 11, 21] check CTL* properties against automata models. The logic is interpreted over “Kripke structures” (see 3.2.1) in order to express model checking algorithms and satisfaction of a state formula is defined in a natural inductive way (see [16] for complete definitions). A Mealy machine can be mapped to a Kripke structure, which is also a state machine.

3.2.1 Verification context

In this section, we formally introduce the temporal logic we consider and its Kripke structure model.

\footnote{It is a weak alarm since lying posture is not dangerous in all contexts.}
Kripke Structure

Kripke structures are verification models against which model-checking algorithms are defined.

A Kripke structure $K$ is a tuple: $K = <Q, Q_0, A, R, L>$ where:

1. $Q$ is a finite set of states
2. $Q_0 \subseteq Q$ is the set of initial states
3. $A$ is a finite set of atomic propositions
4. $R \subseteq Q \times Q$ is a transition relation that must be total: for every state $q \in Q$, there is a state $q'$ such that $R(q, q')$
5. $L : S \mapsto 2^A$ is a labeling function that labels each state by the set of atomic propositions true in that state.

Let $K$ be a Kripke structure, a path in $K$ is an infinite sequence of states: $\pi = q_0, q_1, q_2, \ldots$ such that $\forall i \in \mathbb{N}, R(q_i, q_{i+1})$. Moreover, $\pi^n = q_n$.

From Mealy Machine to Kripke structures

Let $M = <Q, q^{init}, I, O, T, \lambda>$ be a Mealy machine, a terminal state is a state $q \in Q$ such that $\not\exists q \xrightarrow{i/o} q' \in T$. The Kripke structure $K(M)$ associated with $M$ is defined as follows: $K(M) = <Q^K, Q^K_0, A^K, R^K, L^K>$ where

1. $Q^K \subseteq Q \times 2^{A^K} : Q^K = \{(q, v) | \exists q \xrightarrow{i/o} q' \in T \text{ and } \{i\} \cup o = v \} \cup \{(q, \emptyset) | q \in Q\}$.
2. $Q^K_0 = ((q^{init}) \times 2^{A^K}) \cap Q^K$
3. $A^K = IB \cup O\epsilon$
4. $L^K(s, v) = v$
5. $((q, v), (q', v')) \in R^K$ if $\exists q \xrightarrow{i/o} q'$ and $v = \{i\} \cup o$ and $(q', v') \in Q^K$ and $((q, \emptyset), (q, \emptyset)) \in R^K$ for $q \in Q$.

3.2.2 Properties Definition

The logic ($\forallCTL^*$) we consider to express properties is a formal language where assertions related to behavior are easily expressed. It is based on first-order logic but, in order to be efficient when deciding whether a formula is true, the existential path quantifier has been eliminated. It offers temporal operators that make it possible to express properties holding for a given state, for the next state (operator $X$), eventually for a future state ($F$), for all future states ($G$), or that a property remains true until some condition ($U$). We can also express that a property holds for all the paths starting in a given state ($\forall$).

Formally, the logic $\forallCTL^*$ we consider is the set of state formulas defined as follows:

- The constants $true$ and $false$ are state formulas.
• If $p \in A$, $p$ is a state formulas ($A$ is the alphabet of the Kripke structure we consider).
• If $\psi$ and $\phi$ are state formulas, then $\psi \lor \phi$ and $\psi \land \phi$ are state formulas.
• If $\phi$ is a path formula then $\forall(\phi)$ is a state formula.
• If $\phi$ is a state formula then $\phi$ is also a path formula.
• If $\psi$ and $\phi$ are path formulas, then $\psi \lor \phi$ and $\psi \land \phi$ are path formulas.
• If $\psi$ and $\phi$ are path formulas, then so are:
  - $X\phi$
  - $\phi U \psi$

Two abbreviations are used: $F\phi$ and $G\phi$ ($\phi$ is a path formula) respectively denote $true U \phi$.

Satisfaction of formulas

Now, we introduce the notion of “satisfaction of a formula”. Given a Kripke structure $K$ ($K = \langle Q, Q_0, A, R, L \rangle$), the satisfaction of a state formula ($\phi$) by a state $q$ of $K$ (denoted $q \models \phi$) or of a path formula $\psi$ by a path $\pi$ (denoted $\pi \models \psi$) is inductively defined as follows:

- $q \models true$, $q \not\models false$, $q \models p$ iff $p \in L(q)$ and $q \not\models p$ iff $p \notin L(q)$.
- $q \models \psi \lor \phi$ iff $q \models \psi$ or $q \models \phi$, $q \models \psi \land \phi$ iff $q \models \psi$ and $q \models \phi$.
- $q \models \forall(\phi)$ iff for every path $\pi$ starting at $q$, $\pi \models \phi$.
- $\pi \models \phi$ where $\phi$ is a state formula, iff the first state of $\pi$ satisfies $\phi$.
- $\pi \models \psi \lor \phi$ iff $\pi \models \psi$ or $\pi \models \phi$, $\pi \models \psi \land \phi$ iff $\pi \models \psi$ and $\pi \models \phi$.

• If $\psi$ and $\phi$ are path formulas:
  - $\pi \models X\phi$ iff $\pi^1 \models \phi$.
  - $\pi \models \phi U \psi$ iff $\exists n \in \mathbb{N}$ such that $\pi^n \models \psi$ and $\forall i \leq n, \pi^i \models \phi$.

Definition 1:

We say that a Kripke structure $K$ satisfies a state formula $\psi$ ($K \models \psi$) if property $\psi$ is true for the initial states of $K$. This definition is extended to Mealy machines: $M \models \psi$ iff $K(M) \models \psi$.

In our approach, several synchronous monitors can drive the same proxy component, corresponding to several sub assemblies respectively managing different concerns, all of them related to the critical component. For instance, in the application introduced in section ??, there is another assembly associated with a camera sensor also connected to the warning entry of the Alarm component. Thus, we will define another synchronous monitor telling the behavior of this assembly (see figure 3). The output event $warning_1$ of this camera monitor is connected to the warning entry of the Alarm component. Thus, we must specify how we compose the posture monitor and the camera monitor to have the expected behavior of the Alarm component when it receives both $warning_1$ and $warning_3$. 

RR n° 7541
Composition and Formal Validation in Reactive Adaptive Middleware

4 Synchronous Model Composition

4.1 Multiple Access to Components.

When a critical component has multiple synchronous monitors corresponding to several concern managements in the application, we want to build an only synchronous model component which agrees with all these primitive synchronous monitors and whose output event set is related to the input event set of the critical component by an injection. We continue to rely on our use case (see section ??) to illustrate such a situation.

In this use case, there are three sub-assemblies linked to the critical Alarm component. Thus, we introduce three synchronous monitors in this assembly. The first synchronous monitor describes the behavior of Alarm component with respect to the sub assembly managing the camera device; the second is defined with respect to the sub assembly related to the door fridge and timer sensors; and the third tells the behavior of Alarm when it is related to a sub assembly managing a posture detection sensor. camera monitor is described in section 4.1 while posture monitor is in section 3.1.2. The fridge monitor is detailed in figure 4. Then, we get the assembly described in figure 5. We can see that warning and weak_alarm entries have multiple access. Our method will replace these three components by a single component: $\text{camera} \otimes \text{fridge} \otimes \text{posture}$ (see figure 6).

Now we introduce useful definitions to formally specify our composition operation.

Definition 2:
The synchronous product of two Mealy machines $(M_1 \otimes M_2)$ is defined as follows:
Composition and Formal Validation in Reactive Adaptive Middleware

Figure 5: Multiple access to alarm proxy component

Figure 6: Composition of multiple access to connect the alarm proxy component

assume that

\( M_1 =< Q_1, q_1^{init}, I_1, O_1, T_1, \lambda_1 > \) and \( M_2 =< Q_2, q_2^{init}, I_2, O_2, T_2, \lambda_2 > \),

then \( M_1 \otimes M_2 = < Q_1 \times Q_2, (q_1^{init}, q_2^{init}), I_1 \cup I_2, O_1 \cup O_2, T, \lambda > \),

where \( T = \{(q_1, q_2) \mid (q_1', q_2') \in T_1, (q_2', q_2') \in T_2\} \) and

\( \forall (q_1, q_1') \in T_1 \mid \lambda_1((q_1, q_1'), i_1) = o_1 \) and \( \forall (q_2, q_2') \in T_2 \mid \lambda_2((q_2, q_2'), i_2) = o_2 \)

then \( \lambda((q_1, q_2), (q_1', q_2'), i_1, i_2) = o_1 \cup o_2 \).

The synchronous product considers all the combinations of states, taking into account the simultaneity of events according to our synchronous approach. As already mentioned, in the composition operation we consider only synchronous monitors driving the same proxy component. On one hand, the synchronous product allows to agree with each synchronous monitor. On the other hand, it introduce transitions whose output label carry events belonging to the union of the respective output event sets of \( M_1(O_1) \) and \( M_2(O_2) \). But we want that the relationship between the output event set of the composition and the input set of the critical component will be at least an injection. Thus, we apply to the synchronous product a “constraint function” defined according to the respective injections \( i_{1} : O_1 \rightarrow I_C \) and \( i_{2} : O_2 \rightarrow I_C \). First, we introduce a new output event set \( O \) and an injection \( \text{in} : O \rightarrow I_C \). Second, we define a surjective function \( \gamma : O_1 \cup O_2 \cup O_1 \times O_2 \rightarrow O \) such that:

1. \( \forall o_1 \in O_1, \gamma(o_1) = o \) and \( \text{in}(o) = i_{1}(o_1) \)

2. \( \forall o_2 \in O_2, \gamma(o_2) = o \) and \( \text{in}(o) = i_{2}(o_2) \)

From these definitions, a “constraint” function \( \zeta : 2^{O_1 \cup O_2} \rightarrow 2^O \) is deduced:

\( \forall o \in 2^{O_1 \cup O_2} \), if \( \exists o_1, o_2 \in o \) such that \( \gamma(o_1, o_2) \neq \epsilon \) then \( \gamma(o_1, o_2) \in \zeta(o) \); else \( \gamma(o_1) \in \zeta(o) \) and \( \gamma(o_2) \in \zeta(o) \).

This constraint function is applied to the output label sets of the synchronous product:

**Definition 3:**

Assume that \( M_1 \otimes M_2 = < Q_1 \times Q_2, (q_1^{init}, q_2^{init}), I_1 \cup I_2, O_1 \cup O_2, T, \lambda > \), then \( M_1 \otimes \zeta M_2 = < Q_1 \times Q_2, (q_1^{init}, q_2^{init}), I_1 \cup I_2, O, T_\zeta, \lambda_\zeta > \) where \( T_\zeta = T \) and \( \lambda_\zeta \)

RR n° 7541
is defined as follows:
\[ \lambda((q_1, q_2), (q_1', q_2')) = \omega \text{ if } \omega \text{ is an atom in } I_1 \cup I_2. \]

pI1 is defined structurally:
\[ pI1(\omega) = \omega \text{ if } \omega \text{ is an atom in } I_1; \]

The synchronous product of two Mealy machines yields a Mealy machine. It is a well known result of the synchronous framework. Constraint function application modifies only output event sets of labels and thus our composition operation constructs a Mealy machine.

4.2 Composition and Validation.

Our composition operation allows to solve the multiple access to a given proxy component problem. As previously mentioned, we aim at validating critical component behavior. The result of composition operation is a Mealy machine against which model-checking techniques apply as for any synchronous monitor (see 3.2). Moreover, we also want the preservation of properties under composition: if \( M_1 \) verifies an \( \forall C T L^* \) formula \( \Phi (M_1 \models \Phi) \) then this latter also holds for a composition where \( M_1 \) is part of \( (M_1 \otimes M_2) \). To prove such a feature, we show that \( \mathcal{K}(M_1) \) can be viewed as an “approximation” of \( \mathcal{K}(M_1 \otimes M_2) \).

Definition 4:
Let \( K_1 = < Q_1, Q_1^0, A_1, R_1, L_1 > \) and \( K_2 = < Q_2, Q_2^0, A_2, R_2, L_2 > \) be two kripke structures and \( h_\alpha \) a surjection from \( A_1 \) to \( A_2 \). We say that \( K_2 \) approximates \( K_1 \) (denoted \( K_1 \subseteq_h K_2 \)) when

1. It exists a surjection \( h : Q_1 \mapsto Q_2 \) such that: \( h(q_1) = q_2 \Rightarrow \forall a_2 \in L_2(q_2), \exists a_1 \in L_1(q_1) \) and \( h_\alpha(a_1) = a_2. \)
2. \( \forall q_2 \in Q_2^0, \exists q_1 \in Q_1^0 \) and \( h(q_1) = q_2; \) and
3. \( \exists q_1, q_1' (h(q_1) = q_2, h(q_1') = q_2' \text{ and } R_1(q_1, q_1') \Rightarrow R_2(q_2, q_2')). \)

For short, we will denote \( M_1 \otimes M_2 \) as \( M_\alpha \). To benefit from results concerning the preservation of \( \forall C T L^* \) properties through approximations, we want to show that \( \mathcal{K}(M_1) \) is an approximation of \( \mathcal{K}(M_\alpha) \).

4.2.1 Approximations for Synchronous Monitors

\( \mathcal{K}(M_1) = < KQ_1, Q_1^0, A_1, R_1 > \) and \( \mathcal{K}(M_\alpha) = < KQ_\alpha, Q_\alpha^0, A_\alpha, L_\alpha, R_\alpha > \) are built according to the translation operation described in 3.2.1. Our goal is to define a surjective mapping \( h : KQ_\alpha \mapsto KQ_1 \) and to show that it agrees with the definition of approximation (definition4).

We first define a surjective mapping \( h_\alpha \) from \( A_\alpha \) to \( A_1 \). The alphabets of Kripke structures associated with Mealy machines are composed of (1) the Boolean expressions built from inputs and (2) the outputs. Thus, \( h_\alpha \) must be defined on both.

To ease the definition of \( h_\alpha \), we start by defining a projection function \( p_1 \) from \( (I_1 \cup I_2)^B \) to \( I_1^B \). Each element \( i \) in \( (I_1 \cup I_2)^B \) has a normal form and can be written as \( \sum \prod \omega_i \) where each \( \omega_i \) is an atom; i.e either an element of \( I_1 \cup I_2 \) or the negation of an element of \( I_1 \cup I_2 \). \( p_1 \) is defined structurally:
\[ p_1(\omega) = \omega \text{ if } \omega \text{ is an atom in } I_1; \]
Composition and Formal Validation in Reactive Adaptive Middleware

Let \( p_I(\omega) = true \) if \( \omega \) is an atom in \( I_2 \);

\[
p_I(\prod_i \omega_i) = \prod_i p_I(\omega_i)
\]

\[
p_I(\sum_j prod_j) = \sum_j p_I(prod_j)
\]

**Lemma 1:**
For each element of \( (I_1 \cup I_2)^B \) of the form \( i_1.i_2 \) with \( i_1 \) (resp. \( i_2 \)) in \( I_1^B \) (resp. \( I_2^B \)), \( p_I(i_1.i_2) = i_1 \).

**Proof.**

\[
i_1 = \sum_k \prod_i \omega_i \quad \text{where} \quad \omega_i \text{ are atoms in } I_1 \quad \text{and} \quad i_2 = \sum_l \prod_j \alpha_j \quad \text{where} \quad \alpha_j \text{ are atoms in } I_2.
\]

\[
p_I(i_1.i_2) = p_I(\sum_k \prod_i \omega_i \cdot \sum_l \prod_j \alpha_j) = p_I(\sum_k \prod_i \omega_i) \cdot p_I(\sum_l \prod_j \alpha_j).
\]

But \( p_I(\alpha_j) = true \) by definition of the projection function, since \( \alpha_j \) atom in \( I_2 \) and \( p_I(\omega_i) = \omega_i \) since \( \omega_i \) is an atom in \( I_1 \).

Thus \( \sum_k \prod_i p_I(\alpha_j) = true \) and \( p_I(i_1.i_2) = \sum_k \prod_i \omega_i = i_1. \)

According to the translation operation from Mealy machine to Kripke structure, \( K\mathcal{Q}_\zeta \subseteq Q_\zeta \times 2^{A_\zeta} \) and \( A_\zeta = (I_1 \cup I_2)^B \cup O_c \).

More precisely, \( K\mathcal{Q}_\zeta = \{(q_1,q_2),v) | \exists (q_1,q_2) \xrightarrow{i/o} (q_1',q_2') \in T_\zeta \text{ and } v = \{i\} \cup o \} \cup \{(q_1,q_2),\emptyset) | (q_1,q_2) \in Q_\zeta \} \).

Similarly, \( K\mathcal{Q}_1 = \{(q_1,v_1) | \exists q_1 \xrightarrow{i_1/o_1} q_1' \in T_1 \text{ and } v = \{i_1\} \cup o_1 \} \cup \{(q_1,\emptyset) | q_1 \in Q_1 \} \).

First, we define a surjection \( \hat{h}_a A_\zeta \rightarrow A_1 \) as follows: \( \forall i \in (I_1 \cup I_2)^B \), \( \hat{h}_a(i) = p_I(i) \). \( \forall o \in O_c \), \( \hat{h}_a(o) = o_1 \) if \( o = \gamma(o_1) \) and \( \hat{h}_a(\epsilon) = \epsilon \).

To easily express the surjective mapping from \( K\mathcal{Q}_\zeta \) to \( K\mathcal{Q}_1 \), we introduce a function \( p_{O_1} : 2^{O_c} \rightarrow 2^{O_1} \):

\( p_{O_1}(o) = \{o_1 | \exists o_2 \in O_2 \text{ and } \gamma(o_1,o_2) \in o \} \cup \{o_1 | \exists o_2 \in O_2 \text{ and } \gamma(o_1,o_2) \in o \} \). Notice that according to the definition of \( \zeta \), \( p_{O_1}(\zeta(o_1 \cup o_2)) = o_1 \). Indeed, \( \forall o \in O_1 \) either there is \( o' \in o_2 \) such that \( \gamma(o,o') \in \zeta(o_1 \cup o_2) \) then \( o \in p_{O_1}(\zeta(o_1 \cup o_2)) \) or \( \gamma(o) \in \zeta(o_1 \cup o_2) \) and then \( o \in p_{O_1}(\zeta(o_1 \cup o_2)) \).

**Lemma 2:**

\( \mathcal{K}(M_\zeta) \models_h \mathcal{K}(M_1) \)

**Proof.** We prove that the three conditions of definition 4 are satisfied.

(1) The mapping \( \hat{h} : K\mathcal{Q}_\zeta \rightarrow K\mathcal{Q}_1 \) is defined as follows:

\( \hat{h}((q_1,q_2),v) = (q_1,v_1) \) with \( v_1 = \{p_{O_1}(v) | (i \in 2^{(I_1 \cup I_2)^B} \cap v) \cup p_{O_1}(v \cup O_c) \}; \)

\( \hat{h} \) verifies the required property for surjection: if \( \hat{h}((q_1,q_2),v) = (q_1,v_1) \) then \( \forall a \in L_1(q_1,v_1), \exists \alpha_c \in L_c(((q_1,q_2),v) \text{ such that } \hat{h}_a(a_c) = a_1. \)

By definition, \( L_1(q_1,v_1) = q_1 \). If \( a_1 \in v_1 \), then either \( a_1 = i_1 \in I_1^B \) or \( a_1 = i_1 \in O_1 \). Assume \( a_1 = i_1 \), then by definition of \( \hat{h} \), there is \( i \in (I_1 \cup I_2)^B \) such that \( p_I(i) = i_1 \) and by definition also \( h_a(i) = i_1 \) and \( i \in v \) thus \( i \in L_\zeta(((q_1,q_2),v). \)

Otherwise,
\[ a_1 \in o_1 \subseteq O_1 \text{ and from the definition of } \hat{h}, a_1 \in p_{O_1 v} \text{ and then } h_\gamma(a_1, a_2) = a_1 \text{ either there is no such } a_2 \text{ and then } h_\gamma(a_1) = a_1. \]

(2) \( \forall \{q_1, v_1\} \in Q^0_1, \exists \{(q_1, q_2), v\} \in Q^0_2 \) and \( \hat{h}(\{(q_1, q_2), v\}) = \{q_1, v_1\} \). But \( \{q_1, v_1\} \in Q^0_1 \) means that \( q_1 = q^{init}_1 \) and \( \exists q^{init}_1 \xrightarrow{i_1/o_1} q'_1 \in T_1 \) and \( v_1 = \{i_1\} \cup o_1. \)

1. If there is a transition \( q^{init}_2 \xrightarrow{i_2/o_2} q'_2 \in T_2 \), then by construction there is a transition \( (q^{init}_1, q^{init}_2) \xrightarrow{i_1/i_2/(o_1 \cup o_2)} (q'_1, q'_2) \) in \( T_\hat{h}. \)

Thus, \( \{(q^{init}_1, q^{init}_2), \{i_1, i_2\} \cup \zeta(o_1 \cup o_2)\} \) is a state of \( KQ_\zeta \) and an initial state in \( Q^0_\zeta. \)

By definition, \( \hat{h}(\{(q^{init}_1, q^{init}_2), \{i_1, i_2\} \cup \zeta(o_1 \cup o_2)\}) = (q^{init}_1, \{p_{T_1} (i_1, i_2)\} \cup p_{O_1}(\zeta(o_1 \cup o_2))). \)

According to lemma 1, \( p_{T_1} (i_1, i_2) = i_1 \) and we defined \( p_{O_1} \) such that \( p_{O_1}(\zeta(o_1 \cup o_2)) = o_1. \) Thus, \( \hat{h}(\{(q^{init}_1, q^{init}_2), \{i_1, i_2\} \cup \zeta(o_1 \cup o_2)\}) = (q^{init}_1, v_1). \)

2. If there is no transition \( q^{init}_2 \xrightarrow{i_2/o_2} q'_2 \in T_2 \), then there is a transition \( (q^{init}_1, q^{init}_2) \xrightarrow{i_1/o_1} (q'_1, q^{init}_2) \) in \( T_\hat{h}. \) In this last case, the result is obvious.

(3) Consider two states in \( \hat{KQ}_\zeta \), \( \{(q_1, q_2), v\} \) and \( \{(q'_1, q'_2), v'\} \) belonging to the transition relation of \( \hat{K}(M_1) \) and \( \hat{h}(\{(q_1, q_2), v\}) = (q_1, v_1) \) and \( \hat{h}(\{(q'_1, q'_2), v'\}) = (q'_1, v'_1). \)

We want to prove that \( (q_1, v_1) \) and \( (q'_1, v'_1) \) belong to the transition relation of \( \hat{K}(M_1) \). But, there is a transition \( (q_1, q_2) \xrightarrow{i/o} (q'_1, q'_2) \) in \( Q_\zeta \) and \( v = \{i\} \cup o. \) Once again, that means that \( \exists q_1 \xrightarrow{i_1/o_1} q'_1 \in T_1 \) and \( \exists q_2 \xrightarrow{i_2/o_2} q'_2 \in T_2 \) and \( i = i_1, i_2 \) and \( o = \zeta(o_1 \cup o_2). \) Then, \( v_1 = \{i_1\} \cup o_1 \) and by definition \( \{(q_1, v_1), (q'_1, v'_1)\} \in R_1. \)

4.3 Approximation and Property Preservation

Now we make more precise what does mean \( \forall CTL^* \) properties are preserved through our composition operation. In [15], Clarke and all shows that \( \forall CTL^* \) are preserved for transition system approximations. We use the same method to prove that \( \forall CTL^* \) formulas are preserved through Kripke structure approximations.

4.3.1 \( \forall CTL^* \) Property Preservation

Let \( K_1 \) and \( K_2 \) be two Kripke structures and \( h_a \colon A_1 \rightarrow A_2 \) a surjective mapping such that there is a surjection \( h \) from \( Q_1 \) to \( Q_2 \) and \( K_1 \subseteq h K_2. \) The method consists in (1) defining a translation \( \tau \) from formulas expressing properties in \( K_2 \) and formulas expressing properties in \( K_1 \) and to prove that if a property \( \phi \) holds for \( K_2 \), \( \tau(\phi) \) holds for \( K_1 \).

Definition 5:
The translation \( \tau \) between formulas in \( K_2 \) and formulas in \( K_1 \) is defined as follows:

- \( \tau(\text{true}) = \text{true}, \tau(\text{false}) = \text{false} \)

RR n° 7541
• ∀a2 ∈ A2, τ(a2) = {a1 ∈ A1 such that h(a1) = a2};
• if φ and ψ are state formulas, then τ(φ ∨ ψ) = τ(φ) ∨ τ(ψ) and τ(φ ∧ ψ) = τ(φ) ∧ τ(ψ);
• if φ is a path formula, then τ(∀φ) = ∀(τ(φ));
• if φ and ψ are path formulas, then τ(φ ∨ ψ) = τ(φ) ∨ τ(ψ) and τ(φ ∧ ψ) = τ(φ) ∧ τ(ψ);
• if φ and ψ are state formulas, then τ(Xφ) = Xτ(φ) and τ(φ U ψ) = τ(φ) U τ(ψ).

We now turn to the preservation result. First, we express a straightforward lemma that says that paths in $K_1$ are projected in $K_2$ (see [15]).

**Lemma 3:**
If $π = π_1, π_2, π_n, \ldots$ is a path in $K_1$, then $h(π) = h(π_1), h(π_2), \ldots$ is a path in $K_2$.

Relying on this lemma, we prove the preservation theorem:

**Theorem 1:**
Let $K_1$ and $K_2$ two Kripke structures such that $K_1 ⊆ h K_2$:

1. for all ∀CTL* state formula $φ$ in $K_2$ and for all state $q_1$ of $K_1$, $h(q_1) ≡ φ \implies q_1 ≡ τ(φ)$
2. for all ∀CTL* path formula $φ$ in $K_2$ and for every path $π$ in $K_1$, $h(π) ≡ φ \implies π ≡ τ(φ)$

**Proof.** The proof is an induction on the structure of the formula.

1. if $φ = true$ (resp. $false$) the result is obvious;
2. if $φ ∈ L_2(h(q_1))$, by definition, $∃a_1 ∈ L_1(q_1)$ such that $h(a_1) = φ$. Thus $q_1 ≡ a_1$ and then $q_1 ≡ ∨{a_1 ∈ A_1 such that h(a_1) = φ}$. Thus $q_1 ≡ τ(φ)$;
3. if $φ = φ_1 ∨ φ_2$, $h(q_1) ≡ φ_1$ or $h(q_1) ≡ φ_2$. By induction, we know that $q_1 ≡ τ(φ_1)$ or $q_1 ≡ τ(φ_2)$. Thus $q_1 ≡ τ(φ_1) ∨ τ(φ_2)$ and $q_1 = τ(φ)$. The proof for $∧$ is similar;
4. assume $φ = ∀ψ$, we want to prove that $q_1 ≡ τ(∀ψ)$. This means that for every path $π$ starting from $q_1 q_1 ≡ ψ$. From lemma 3, we know that $h(π)$ is a path in $K_2$ starting from $h(q_1)$. Since $h(q_1) ≡ ∀ψ$, $h(π) ≡ ψ$. Applying the induction hypothesis, we deduce that $π ≡ τ(ψ)$;
5. if $φ$ is a state formula and $h(π) ≡ φ$. If the initial state of $π$ is $q_1$, then the initial state of $h(π)$ is $h(q_1)$. Assume that $h(q_1) ≡ φ$, then by induction $q_1 ≡ τ(φ)$ and thus $π ≡ τ(φ)$;
6. the proofs for $∧$ and $∃$ of path formulas are similar to case (3);
7. if $h(π) ≡ Xψ$ then $h(π)^1 ≡ ψ$. By induction, $π^1 ≡ τ(ψ)$ thus $π ≡ Xτ(ψ)$ and $π ≡ τ(Xψ)$;
8. if \( h(\pi) \models \phi U \psi \), there is \( n \in \mathbb{N} \) such that \( h(\pi)^n \models \psi \) and \( \forall i < n, h(\pi)^i \models \phi \).

Using the induction hypothesis, we can infer that \( \pi^n \models \tau(\psi) \) and \( \forall i < n, \pi^i \models \tau(\phi) \). Thus \( \pi \models \phi U \psi \).

\qed

4.3.2 Properties Preservation for Synchronous Monitors

Now, we apply these preservation results to synchronous monitors. We recall that we want to prove that if a Mealy machine \( M_1 \) satisfies a \( \forall CTL^* \) formula, then the property holds also in a composition where \( M_1 \) is an argument. To this aim, relying on theorem 1, we will show that if \( \mathcal{K}(M_1) \models \tau(\phi) \), \( \tau \) being a translation function from formulas related to \( \mathcal{K}(M_1) \) to formulas related to \( \mathcal{K}(M_\zeta) \).

**Definition 6:**

The translation mapping \( \tau_\zeta \) between formulas related to \( \mathcal{K}(M_\zeta) \) and those related to \( \mathcal{K}(M_1) \) is defined as follows:

- \( \tau_\zeta(true) = true \), \( \tau_\zeta(false) = false \);
- \( \forall a_1 \in A_1, \tau_\zeta(a_1) = \sqrt{\{a_\zeta \in A_\zeta \text{ such that } \hat{h}_a(a_1) = a_\zeta\}} \);
- if \( \phi \) and \( \psi \) are state formulas, then \( \tau_\zeta(\phi \lor \psi) = \tau_\zeta(\phi) \lor \tau_\zeta(\psi) \) and \( \tau_\zeta(\phi \land \psi) = \tau_\zeta(\phi) \land \tau_\zeta(\psi) \);
- if \( \phi \) is a path formula, then \( \tau_\zeta(\forall \phi) = \forall(\tau_\zeta(\phi)) \);
- if \( \phi \) and \( \psi \) are path formulas, then \( \tau_\zeta(\phi \lor \psi) = \tau_\zeta(\phi) \lor \tau_\zeta(\psi) \) and \( \tau_\zeta(\phi \land \psi) = \tau_\zeta(\phi) \land \tau_\zeta(\psi) \);
- if \( \phi \) and \( \psi \) are state formulas, then \( \tau_\zeta(X\phi) = X\tau_\zeta(\phi) \) and \( \tau_\zeta(\phi U \psi) = \tau_\zeta(\phi) U \tau_\zeta(\psi) \).

Now we can express the preservation theorem for synchronous monitors:

**Corollary 1:**

Let \( M_1 \) and \( M_2 \) be two Mealy machines and \( \phi \) a \( \forall CTL^* \) formula related to \( M_1 \), then \( M_1 \models \phi \Rightarrow M_1 \otimes \mid_\zeta M_2 \models \tau_\zeta(\phi) \).

**Proof.** By definition, we say that \( M_1 \models \phi \) if and only if \( q_1^{init} \models \phi \) and \( (q_1^{init}, v_1) \models \phi \) for each initial states of \( \mathcal{K}(M_1) \). In section 4.2.1, we have defined a surjective mapping \( \hat{h} : \mathcal{K}Q_\zeta \mapsto \mathcal{K}Q_1 \) and we have proved that \( \mathcal{K}(M_\zeta) \subseteq \hat{h}(\mathcal{K}(M_1)) \). Let us consider the state \( \{(q_1^{init}, q_2^{init}), v\} \) such that \( \hat{h}(\{(q_1^{init}, q_2^{init}), v\}) = (q_1^{init}, v_1) \), we have \( \hat{h}(\{(q_1^{init}, q_2^{init}), v\}) \models \phi \) as initial hypothesis. Thus, according to theorem 1, we know that \( \{q_1^{init}, q_2^{init}\} \models \tau_\zeta(\phi) \). Hence, \( M_\zeta \models \tau_\zeta(\phi) \). \qed

5 Practical Issues

Relying on this theoretical approach, we improve our \( WComp \) middleware to support synchronous component design and validation of behaviors for critical components.
5.1 Our Reactive Adaptive Middleware

As already mentioned in the introduction, we propose a middleware approach called WComp taking into account all the principles for ubiquitous computing detailed in section 1.1. For that matter, it federates three main paradigms:

1. **Event-based services architecture**: Our services are event-based. They can communicate between them using event patterns to transmit as soon as possible spontaneous information coming from the physical environment. For example, we attach a service to a sensor device that sends regularly new measures to other services. They are generally Web Services for Devices like UPnP or DPWS. We distinguish then two kinds of services: composite services which are services whose implementation calls other services in the middleware layers. They are opposed to basic services from the infrastructure, whose implementation is self-contained and does not invoke any other services. Ubiquitous applications are then a graph of interactions between event-based services.

2. **Lightweight component-based architecture inside composite web services**: A Composite Service is based on an internal lightweight component assembly to manage composition between other event-based web services through proxies components and to design the interface of a new higher-level composite service. A Composite Service corresponds to a dynamic assembly of lightweight WComp components and provides an event-based service interfaces, like explained previously. Internal assembly of components handles the high dynamicity of the model, providing a way to be structurally modified and adapted. It also addresses reactivity, since it uses event-based communications between components. A composite event-based service is dynamically managed using an internal lightweight components assembly.

3. **Adaptation paradigm using the original concept named Aspect of Assembly (AA)**: This concept allows to prepare kinds of independent and crosscutting schemes of adaptation dealing with separation of concerns, logically mergeable in case of conflicts and applicable to every Composite Web Service of the application, not necessarily known (previously). Aspects provide adaptation to the model, which is structural, since we modify the internal component assembly of composite services, without modifying black boxes components. Adaptations as a set of AA, are designed to modify event-based web services of the application according to the evolution of the infrastructure (appearance and disappearance of devices in it). They are applied (weaved) to the set of event-based composite web services of the applications at runtime to implement then required reactive adaptation.

Thus our middleware allows to adopt both ways to dynamically design ubiquitous computing applications. The first implements a classical component-based compositional approach, using SLCA, to design higher-level composite web services and then increments the graph of cooperating services for the applications. This approach is well suited to design the applications in a known, common and usual way. We call such a compositional approach composition for higher-level services.
The other way uses a compositional approach for adaptation using AA, particularly well-adapted to tune a set of event-based web services in reaction to a particular variation of the context. We call such compositional approach composition for reactive adaptation.

5.2 Extending WComp

In section 3, we have shown that the introduction of specific synchronous component is an answer to address the multiple access to critical component problem. These synchronous component we introduce represent the behaviors of critical components as Mealy machines. These latter are models very well suited to perform safety property verification, but they are not convenient to deal with. Due to the synchronous product they can become huge and we must face the famous “state explosion problem”. To avoid this drawback, we want to benefit from symbolic representation of Mealy machines. Thus we rely on synchronous languages [2]. These languages support functional concurrency and they rely on notations that express concurrency in a user-friendly manner. They also offer simple formal model that makes formal reasoning tractable. In particular, the semantics for the parallel composition of two processes is clearly defined. Finally, they respect the synchrony hypothesis which divides time into discrete instants. Hence in a natural way, synchronous programs progress according to successive atomic reactions. Indeed, Mealy machines are models for these languages and their compilation involves the construction of these formal models. Moreover, synchrony and concurrency imply that the synchronous product defined section 4 is exactly the semantics of parallel operator of synchronous languages.

Then, to apply our approach, we rely on the Lustre [19] synchronous language which helps us to define and validate synchronous components. It is a data flow language offering two main advantages: (1) It is a functional language no complex side effects. This makes it well adapted to formal verification and safe program transformation, since functional relations over data flows may be seen as time invariant properties. Also, reuse is made easier, which is an interesting feature for reliable programming concerns; (2) it is a parallel model, where any sequencing and synchronization depends on data dependencies. Thus, the synchronous product we rely on to perform the composition of synchronous components under constraints is expressed naturally in the language. Indeed, constraint functions can be expressed as equations, thanks to the equational nature of the language.

To perform safety properties validation we rely on the model-checking tool Lesar [10], a symbolic, BDD-based model-checker for Lustre. It is based on the use of synchronous observers [9], to describe both the properties to be checked and the assumptions on the program environment under which these properties are intended to hold. An observer of a safety property is a program, taking as inputs the inputs/outputs of the program under verification, and deciding (e.g., by emitting an alarm signal) at each instant whether the property is violated. Running in parallel with the program, an observer of the desired property, and an observer of the assumption made about the environment one has just to check that either the alarm signal is never emitted (property satisfied) or the alarm signal is emitted (assumption violated), which can be done by a simple traversal of the reachable states of the compound program. Hence, using
observer technique allows to express the property in the same language used to
design our synchronous components and avoid to express non intuitive temporal
logic formulas.

5.3 Use Case Implementation

Now we sketch how we implement the use case described in section ???. In
our implementation, a synchronous monitor is expressed as a Lustre program
(called a node). Hence three Lustre nodes implement respectively the three
synchronous monitors of the use case:

\begin{verbatim}
node camera(in_kitchen, close_fridge:bool) returns(warning1:bool)
  let warning1 = in_kitchen and close_fridge;
node fridge(fridge_opened, one_minute: bool)
  returns (warning2, weak_alarm2: bool);
  let warning2= fridge_opened and not one_minute;
  weak_alarm2= fridge_opened and one_minute;
node posture(sitting, standing, lying:bool)
  returns(warning3, weak_alarm3:bool)
  let warning3 = (standing or sitting) and not lying;
  weak_alarm3 = not standing and not sitting and lying;

Figure 5 shows the assembly weaved to design the application. Let \( O_1 = \{\text{warning}_1\} \), \( O_2 = \{\text{weak}\_\text{alarm}_2, \text{warning}_2\} \) and
\( O_3 = \{\text{weak}\_\text{alarm}_3, \text{warning}_3\} \) be the respective output sets of \textit{camera, fridge} and \textit{posture} components.

Let \( I_A = \{\text{warning, weak}\_\text{alarm, strong}\_\text{alarm}\} \) be the input set of the \textit{Alarm}
component.

For each component, we defined an injection \( \text{in}_i : O_i \mapsto \text{I}_A(i = 1, 2, 3) \):

\[
\left\{ \begin{array}{l}
\text{in}_i(\text{warning}_i) = \text{warning}(i = 1, 2, 3) \\
\text{in}_i(\text{weak}\_\text{alarm}_i) = \text{weak}\_\text{alarm}(i = 2, 3)
\end{array} \right.
\]

Thus \textit{warning} and \textit{weak\_alarm} entries have multiple access. We will replace the
three components by a single component \( \text{camera} \otimes \text{fridge} \otimes \text{posture} \mid \zeta \). As de-
scribed in section 4, this composite component is a Mealy machine, which has for
input event set the union of the respective input event sets of the \textit{camera, fridge} and \textit{posture} components i.e \{\text{close\_fridge, in\_kitchen, fridge\_opened, one\_minute, standing, sitting, lying}\}. The output set of the composite component we built
is \{\text{warning, weak\_alarm, strong\_alarm}\} (we will call it \( O \)). As it is in bi-
jection with the input set of \textit{Alarm} component, we keep the same name to an
easier identification of connections. Now, we must provide a surjective function
\( \gamma : O_1 \cup O_2 \cup O_3 \cup (O_1 \times O_2 \times O_3) \cup (O_1 \times O_2) \cup (O_2 \times O_3) \cup (O_1 \times O_2) \mapsto O \)
which agrees with the respective injections \( \text{in}_i \mapsto I_A \).

\[
\left\{ \begin{array}{l}
\gamma(\text{warning}_i) = \text{warning}(i = 1, 2, 3) \\
\gamma(\text{weak}\_\text{alarm}_i) = \text{weak}\_\text{alarm}(i = 2, 3) \\
\gamma(\text{weak}\_\text{alarm}_2, \text{weak}\_\text{alarm}_3) = \text{strong}\_\text{alarm}
\end{array} \right.
\]

otherwise \( \gamma(o) = \epsilon \)

Then we infer a constraint function \( \zeta : 2^{O_1 \cup O_2 \cup O_3} \mapsto 2^O \) and we apply it to
build the composite component \( \text{camera} \otimes \text{fridge} \otimes \text{posture} \mid \zeta \). The constraint
function applies to the output sets borne by transitions of camera, fridge and posture synchronous product. It maps all combinations of warning1, warning2 and warning3 to warning event. As soon as either weak_alarm2 or weak_alarm3 are emitted, ζ maps the output set to weak_alarm and if both of them belong to an output set, then a strong_alarm is sent since that means that the door of the fridge is opened for more than one minute and the tracked person is lying. Of course, different constraints could be defined. For instance, instead of considering that a warning1 is sufficient to launch a warning, we could consider that the camera and fridge components must agree and emit respectively warning1 and warning2. This would yield another composition result.

To implement the synchronous monitor performing the composition of camera, fridge and posture synchronous monitors, we rely on the natural synchronous parallelism of Lustre. Indeed in this language, the synchronous product is implicit and we only have to call the respective nodes implementing the components to build their synchronous product. Then, to express the constraint function, we define a set of equations describing the computation of each output of the composition (showing in violet in the following):

```
node alarm_comp (close_fridge, fridge_opened, one_minute, standing, sitting, lying, in_kitchen : bool)
  returns (warning, weak_alarm, strong_alarm : bool)
var warning1, warning2, warning3, weak_alarm2, weak_alarm3 : bool;
let warning1 = camera(in_kitchen, close_fridge);
(warning2, weak_alarm2) = fridge(fridge_opened, one_minute);
(warning3, weak_alarm3) = posture(standing, sitting, lying);

warning = warning1 or warning2 or warning3 and not weak_alarm2 and not weak_alarm3;
weak_alarm = weak_alarm2 xor weak_alarm3;
strong_alarm = weak_alarm2 and weak_alarm3;
```

tel

Now, we want to verify the alarm_comp node behavior before introducing it in the assembly. Thus, we use the observer technique previously described to prove that if the fridge is opened for more than one minute and the person is lying, then a strong alarm is sent. To this aim, we define the following verif node. It listens all the entries the alarm_comp node listens and it computes a Boolean output prop. Then the model checker Lesar verifies that prop is always true, assuming that standing, sitting and lying are exclusive.

```
node verif (close_fridge, fridge_opened, one_minute, standing, sitting, lying, in_kitchen : bool) returns (prop: bool)
var warning, weak_alarm, strong_alarm : bool;
let (warning, weak_alarm, strong_alarm) = alarm_comp(close_fridge, fridge_opened, one_minute, standing, sitting, lying, in_kitchen);
assert (not ((standing and lying) or (standing and sitting) or (lying and sitting)));

prop = if (fridge_opened and one_minute and lying) then strong_alarm else true;
tel
```

On another hand, we just want to touch on the application of property 1. Assume that with Lesar, we prove that for fridge component, the property: fridge_opened ⇒ warning2 holds. Clearly, from the definition of constraints
In alarm\_comp, we have $\zeta(\text{warning2}) = \text{warning}$. Thus, we can deduce that fridge\_opened $\Rightarrow$ warning also holds in alarm\_comp.

After this verification, we automatically generated WComp input code for node comp. Thus this new component has been automatically weaved in the assembly designing the application in WComp. Figure 7 shows the resulting assembly.

6 Related Works

In this work, we rely on a synchronous modelling to verify the functional correctness under concurrency of component behavior and component assemblies in a reactive and adaptive middleware. Indeed, only few research works in ubiquitous
computing address some partly critical applications. For example CORTEX [26] proposes a model of sentient object to address the emergence of a new class of application that operate independently of human control. The corresponding middleware has to cope with applications that are critical in time and safety. Amigo [14] middleware platform deal with safety-related services and then assign them with higher priority than other services. Anyway if such middleware identify the problem, they don’t adopt a specific approach with specific tools for that. On another hand, some works address the reliability of middleware. For instance, in [25], the authors propose the TLAM (two-level actor model) approach for specifying and reasoning about components of open distributed systems. They show, using the QoS broker MM architecture, how the TLAM framework can be used to specify and reason about distributed middleware services and their composition. They have also shown how specifications in the TLAM framework can lead to implementations. They proved that the implemented middleware correctly works (provided that middleware services respect a set of constraints) and they planned to rely on a theorem prover to achieve these proofs and automate their method.

However, in the same vein as our approach, some works rely on model-checking techniques to ensure the reliability of middleware solutions. For instance, PolyORB is a schizophrenic (“strongly generic”) middleware offering several core functions and a Broker design pattern to coordinate them. In [13], Hugues and al, generate Petri nets to model the Broker design pattern of PolyORB and use model checking techniques relying on Petri nets models to verify qualitative properties (deadlock, bounds of buffers, appropriate use of critical section,...). We don’t use such a modelling because (1) we want to rely on a user-friendly method to describe critical unknown component behaviors; (2) properties we consider don’t require Petri nets modelling to be checked. Thus, we prefer to rely on a language allowing to express both component behavior and properties to be checked. The work presented in [3] is close to our approach, but is not applied in the same context. The authors present a compositional reasoning to verify middleware-based Software Architecture. They take advantage of the particular structure of applications due to their middleware-based approach to apply the “assume-guarantee” paradigm in their verification process. In this paradigm the validation of a global property is reduced to the verification of local properties against sub components. Properties decomposition is a very hard problem and they propose an automatic means to achieve this decomposition. Our goal is different and surely less ambitious. We are interested to verify only local critical component or assemblies. Following our philosophy, we want to prove properties on the behavior of small entities and thus only a preservation of property validation through a composition operation is relevant for our approach. In [7], Delaval and all also use a synchronous data flow language complemented with a mechanism to depict component contracts (BZR) to extend a high level component-based model (Fractal) in order to enforce safety properties concerning component interactions during dynamic reconfiguration. Indeed from Fractal specification it is possible to extract a BZR program made of the automata representation of the component behavior and the component contract. Then, using an ad-hoc discrete controller synthesis tool, they generate in the target executive middleware of Fractal (C, Java) an additional validated controller. But, at component-based middleware level as WComp is, we have no facilities to deduce component behaviors and constraints. Then, we solve the
problem of safe reconfiguration in relying on the composition under constraint of user-defined synchronous monitors. Moreover, this operation preserves component properties already proved. Finally, we want to mention Shin Nakajima [20] work which shows that model-checking techniques are well suited to verify the reliability of web service flows. He relied on SPIN model-checker [11] to verify the reliability of web service flows expressed as WSFL descriptions. The properties validated are reachability, dead-lock freedom or application specific progress properties.

7 Conclusion and Future Works

The work described in this paper is derived from our experience in providing support for correct assembly of components in an event-based reactive and adaptive middleware. In this latter, we solved the adaptation paradigm using the Aspect of Assembly concept. When using our middleware, a developer benefits from a composition mechanism between different component assemblies to adapt his application to context change. While defining this composition mechanism, we realized the need to formalize and verify the multiple access to a critical component (i.e related to a critical device). The corresponding formalism, the topic of this paper, relies on formal methods. Our approach introduces in a main assembly, a synchronous component for each sub assembly connected with a critical component. This additional component implements a behavioral model of the critical component and model checking techniques apply to verify safety properties about it. Thus, we consider that the critical component is validated. Then we proposed a sound (with respect to our mathematical formalism) composition operation between synchronous components. We proved that this operation preserves already separately verified properties of synchronous components. This operation is an answer to the multiple access to critical components. Our aim is to improve our middleware WComp with a dedicated tool. Currently, we supply a graphical interface to design both critical component behaviors and properties as observers in the synchronous language Lustre (see section 5). Then the validation of properties and the creation of the validated synchronous component is automatic. But, designing with Lustre language is not obvious for any expert user and in the future we aimed at providing a user-friendly interface to express critical component behaviors and properties. This interface will report about violation of properties relying on powerful model checker as NuSMV [5] and straightly (without using the Lustre compiler) generate internal code to implement synchronous monitors.

From a theoretical point of view, we aim at improving the efficiency of the composition mechanism. Instead of replacing synchronous components by their composition, we want to supply a composition synchronous monitor listening the output events of the original synchronous monitors and achieving their composition. Then we must prove that this assembly yields to the same result than to perform the composition under constraints of synchronous monitors. On another hand, a hard and long term challenge is to take into account uncertainty in critical component modelling. Indeed, in some applications, some sensor devices could deliver non accurate information. Then, it would be more realistic to study others models in order to model behavior of critical component when they intervene in an assembly listening an uncertain context. Only few approaches
in synchronous domain offer this feature and model-checking techniques which consider timed or stochastic automata as models are nowadays non efficient.

References


