A Semantic Theory of the Internet of Things [*]

Ruggero Lanotte
Dipartimento di Scienza e Alta Tecnologia
Università degli Studi dell'Insubria, Como, Italy

Massimo Merro
Dipartimento di Informatica
Università degli Studi di Verona, Italy

We propose a process calculus for modelling and reasoning on systems in the *Internet of Things* paradigm. Our systems interact both with the physical environment, via *sensors* and *actuators*, and with *smart devices*, via short-range and Internet channels. The calculus is equipped with a standard notion of labelled *bisimilarity* which is proved to be a coinductive characterisation of a well-known contextual equivalence. We use our semantic proof-methods to prove run-time properties of a non-trivial case study as well as system equalities.

1 Introduction

In the *Internet of Things* (IoT) paradigm, *smart devices* equipped with embedded technology automatically collect information from shared resources (e.g. Internet accesses, physical devices, etc.) and aggregate them to provide new services to end users [18]. The "things" commonly deployed in IoT systems are: *RFID tags*, for unique identification, *sensors*, to detect physical changes in the environment, and *actuators*, to pass information to the environment. To provide proper communication capabilities, smart devices are organized in networks which are based on the standard communication protocol of the Internet framework.

The range of IoT applications is rapidly increasing and already covers several domains [4, 18, 32]: (i) environmental monitoring, (ii) healthcare, (iii) personal and social, (iv) security and surveillance, (v) smart environment (home, offices, cities), (vi) transportation and logistics (automotive).

The research on IoT is currently focusing on practical applications such as the development of enabling technologies [36], ad hoc architectures [34], semantic web technologies [11], and cloud computing [18]. However, as pointed out by Lanese et al. [22], there is a lack of research in formal methodologies to model the interactions among system components, and to verify the correctness of the network deployment before its implementation.

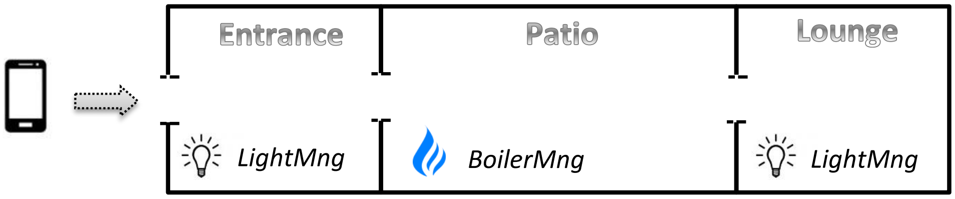
The main goal of the current paper is to propose a new process calculus for IoT systems which supports a clear semantic theory for specifying and reasoning on IoT applications. Devising a calculus for modelling a new paradigm requires understanding and distilling, in a clean algebraic setting, the basic features of the paradigm. In order to point out the main ingredients of the IoT paradigm, we use a small example within the smart environment domain.

Suppose a simple *smart home* (see Figure 1) in which the user can (i) profit of her smartphone to remotely control the heating boiler of her house, and (ii) automatically turn on lights when entering a room. The house consists of an entrance and a lounge, separated by a patio. Entrance and lounge have their own lights (actuators) which are governed by different light manager processes, *LightMng*. The boiler is placed in the patio and it is governed by a boiler manager process, *BoilerMng*. This process senses the local temperature (via a sensor) and decides whether the boiler should be turned on/off, setting a proper actuator to signal the state of the boiler. The smartphone executes two concurrent processes: *BoilerCtrl* and *LightCtrl*. The first one reads user's commands, submitted via the phone touchscreen (a

[*] An extended abstract appeared in the proc. of COORDINATION 2016, LNCS 9686, pp. 157-174, Springer [25].

Submitted to:
Information and Computation

Figure 1 A simple smart home



sensor), and forward them to the process *BoilerMng* of the house, via an Internet channel. Whereas, the process *LightCtrl* interacts with the processes *LightMng* of the house, via short-range wireless channels (e.g. Bluetooth, infrared, etc), to automatically turn on lights when the smartphone physically enters either the entrance or the lounge.

The whole system is given by the parallel composition of the smartphone (a mobile device) and the smart home (a stationary entity).

On this kind of systems one may wish to prove interesting *run-time properties*. Think of a *fairness property* saying that the boiler will be eventually turned on/off whenever specific conditions are satisfied. Or *consistency properties*, saying the smartphone will never be in two rooms at the same time. Even more, one may be interested in understanding whether our system has the same *observable behaviour* of another system. Consider a variant of our smart home, where lights functionality depends on the GPS coordinates of the smartphone (localisation is a common feature of today smartphones). Intuitively, the smartphone could send its GPS position to a centralised light manager, *CLightMng* (possibly placed in the patio), via an Internet channel. The process *CLightMng* will then interact (via short-range channels) with the local light manager processes to turn on/off lights, depending on the current position of the smartphone. Here comes an interesting question: can these two implementations of the smart home, based on different light management mechanisms, be actually distinguished by an end user?

In the paper at hand we develop a fully abstract semantic theory for a process calculus of IoT systems, called `CaIT`. We provide a formal notion of when two systems in `CaIT` are indistinguishable, in all possible contexts, from the point of view of the end user. Formally, we adopt the approach of [20, 37], often called *reduction (closed) barbed congruence*, which relies on two crucial concepts: a *reduction semantics* to describe system computations, and *basic observables* to represent what the environment can directly observe of a system. As IoT systems are essentially *cyber-physical systems* [38], they have at least two possible observables: the ability to transmit along channels, *logical observation*, and the capability to diffuse messages via actuators, *physical observation*. In `CaIT`, we have adopted the second form of observable as our contextual equality remains invariant when adding logical observation. However, the right definition of physical observation is far from obvious as it has a non-trivial impact on the definition of the reduction semantics. Thus, observables and reduction semantics contain *key design choices* for the formal definition of `CaIT`.

Our calculus is equipped with two *labelled transition semantics* (LTSs) in the SOS style of Plotkin [35]: an *intensional* semantics and an *extensional* semantics. The adjective intensional is used to stress the fact that the actions here correspond to activities which can be performed by a system in isolation, without any interaction with the external environment. While, the extensional semantics focuses on those activities which require a contribution of the environment. Our extensional LTS builds on the intensional one, by introducing specific transitions for modelling all interactions with the environment. Here, we would like

Table 1 Syntax

Network:			
M,N	$::=$	$\mathbf{0}$	empty network
	$\mid$	$n[\mathcal{I} \bowtie P]^{\mu}_{h}$	node/device
	$\mid$	$M \mid N$	network composition
	$\mid$	$(\nu c)M$	channel restriction
Process:			
P,Q	$::=$	nil	termination
	$\mid$	$\rho.P$	intra-node activity
	$\mid$	$P \mid Q$	parallel composition
	$\mid$	$\lfloor \pi.P \rfloor Q$	communication with timeout
	$\mid$	$[b]P;Q$	conditional
	$\mid$	X	process variable
	$\mid$	$\mathsf{fix}X.P$	recursion

to point out that since our basic observation on systems does not involve the recording of the passage of time, this has to be taken into account extensionally.

We prove that the reduction semantics coincides with the intensional semantics (Harmony theorem), and that they satisfy some desirable time properties such as *time determinism*, *patience*, *maximal progress* and *well-timedness* [19]. However, the main result of the paper is that *weak bisimilarity* in the extensional LTS provides a *coinductive characterisation* of our contextual equivalence, reduction barbed congruence: two systems are related by some bisimulation in the extensional LTS if and only if they are reduction barbed congruent. Full abstraction results of this kind are in general hard to achieve. In our case, this result required a non-standard proof of the congruence theorem for the weak bisimilarity.

We finally show the effectiveness of our bisimulation proof-technique to deal with non-trivial systems. In particular, we provide a formal proof that two different implementations of the smart home mentioned before are bisimilar. Formal proofs of systems of such size are quite rare in the literature. Thus, in order to reduce the size of the bisimulation relation to be exhibited, we make an intensive use of *up-to expansion* proof-techniques [37].

Outline Section 2 contains the calculus together with the reduction semantics, the contextual equivalence, and a discussion on design choices. Section 3 gives the details of our smart home example, and proves desirable run-time properties for it. Section 4 defines both intensional and extensional LTSs. In Section 5 we define bisimilarity for IoT-systems, and prove the full abstraction result together with a number of non-trivial system equalities. Section 6 discusses related work, and concludes.

2 The calculus

In Table 1 we give the syntax of our *Calculus of the Internet of Things*, shortly `CaIT`, in a two-level structure: a lower one for *processes* and an upper one for *networks* of smart devices. We use letters n,m to denote *nodes/devices*, c,g for *channels*, h,k for (physical) *locations*, s,s' for *sensors*, a,a' for *actuators* and x,y,z for *variables*. Our *values*, ranged over by v and w, are constituted by basic values, such as booleans and integers, sensor and actuator values, and coordinates of physical locations.

A network is a pool of *distinct nodes* running in parallel. Nodes live in a physical world which can be divided in an enumerable set of physical locations. We assume a discrete notion of *distance* between two locations h and k, i.e. $\mathrm{d}(h,k) \in \mathbb{N}$. We write $\mathbf{0}$ to denote the empty network, while $M \mid N$ represents the parallel composition of two networks M and N. In $(\nu c)M$ channel c is private to the nodes of M. Each node is a term of the form $n[\mathscr{I} \bowtie P]^{\mu}_{l}$, where n is the device ID; $\mathscr{I}$ is the physical interface of n, represented as a partial mapping from sensor and actuator names to physical values; P is the process modelling the logics of n; l is the physical location of the device; $\mu \in \{\mathtt{s},\mathtt{m}\}$ is a tag to distinguish between stationary and mobile nodes.

For security reasons, in a node $n[\mathscr{I} \bowtie P]^{\mu}_{h}$, sensors belonging to the physical interface $\mathscr{I}$ can be read only by the corresponding *controller process* P. Similarly, actuators in $\mathscr{I}$ can be modified only by P. No other devices can access the physical interface of n. P is a timed concurrent process which manages both the interaction with the physical interface $\mathscr{I}$ and channel communication with other devices. The communication paradigm is *point-to-point* via channels that may have different transmission ranges. We assume a global function rng() that given a channel c returns an element of $\mathbb{N} \cup \{-1,\infty\}$. Thus, a channel c can be used for: (i) *intra-node communications*, if $\mathrm{rng}(c) = -1$; (ii) *short-range inter-node communications* (such as Bluetooth) if $0 \leq \mathrm{rng}(c) < \infty$; (iii) *Internet communications*, if $\mathrm{rng}(c) = \infty$.

Our processes build on Hennessy and Regan's TPL [19] (basically, CCS with a discrete notion of time). We write $\rho.P$, with $\rho \in \{\sigma, @(x), s?(x), a!v\}$, to denote intra-node actions. The process $\sigma.P$ sleeps for one time unit. The process $@(x).P$ gets the current location of the enclosing node. Process $s?(x).P$ reads a value v from sensor s. Process $a!v.P$ writes the value v on the actuator a. We write $\lfloor \pi.P \rfloor Q$, with $\pi \in \{\overline{c}\langle v \rangle, c(x)\}$, to denote channel communication with timeout. This process can communicate along some channel c and, after that, it continues as P; otherwise, after one time unit, it evolves into Q. The process $[b]P;Q$ is the standard conditional construct, where b is a decidable guard. As in CCS, we assume that $[b]P;Q = P$ if $[\![b]\!] = \mathsf{true}$ (i.e. b evaluates to true), and $[b]P;Q = Q$ if $[\![b]\!] = \mathsf{false}$. In processes of the form $\sigma.Q$ and $\lfloor \pi.P \rfloor Q$ the occurrence of Q is said to be *time-guarded*. The process $\mathsf{fix}X.P$ denotes *time-guarded recursion*, as all occurrences of the process variable X may only occur time-guarded in P. In processes $\lfloor c(x).P \rfloor Q$, $s?(x).P$ and $@(x).P$ the variable x is said to be bound. Similarly, in process $\mathsf{fix}X.P$ the process variable X is bound. In the term $(\nu c)M$ the channel c is bound. This gives rise to the standard notions of *free/bound (process) variables*, *free/bound channels*, and *α-conversion*. A term is said to be *closed* if it does not contain free (process) variables, although it may contain free channels. We always work with closed networks: the absence of free variables is preserved at run-time. We write $T\{^{v}/_{x}\}$ for the substitution of the variable x with the value v in any expression T of our language. Similarly, $T\{^{P}/_{X}\}$ is the substitution of the process variable X with the process P in T.

Actuator names are metavariables for actuators like *display@n* or *alarm@n*. As node names are unique so are actuator names: different nodes have different actuators. The sensors embedded in a node can be of two kinds: *location-dependent* and *node-dependent*. The first ones sense data at the current location of the node, whereas the second ones sense data within the node, independently on the node's location. Thus, node-dependent sensor names are metavariables for sensors like *touchscreen@n* or *button@n*; whereas a sensor *temp@h*, for external temperature, is a typical example of location-dependent sensor. Like actuators, node-dependent sensor names are unique. This is not the case of location-dependent sensor names which may appear in different nodes. For simplicity, we use the same metavariables for both kind of sensors. When necessary we will specify the type of sensor in use.

The syntax given in Table 1 is a bit too permissive with respect to our intentions. We could rule out ill-formed networks with a simple type system. For the sake of simplicity, we prefer to provide the following definition.

Definition 1. *A network M is said to be* well-formed if *(i) it does not contain two nodes with the same name; (ii) different nodes have different actuators; (iii) different nodes have different node-dependent sensors; (iv) for each $n[\mathscr{I} \bowtie P]^{\mu}_{h}$ in M, with a prefix $s?(x)$ (resp. $a!v$) in P, $\mathscr{I}(s)$ (resp. $\mathscr{I}(a)$) is defined; (v) for each $n[\mathscr{I} \bowtie P]^{\mu}_{h}$ in M with $\mathscr{I}(s)$ defined for some location-dependent sensor s, it holds that $\mu = \mathtt{s}$.*

Table 2 Structural congruence

Processes:

$P \mid \mathsf{nil} \equiv P$

$P \mid Q \equiv Q \mid P$

$(P \mid Q) \mid R \equiv P \mid (Q \mid R)$

$[b]P;Q \equiv P$ if $[\![b]\!] = \mathsf{true}$

$[b]P;Q \equiv Q$ if $[\![b]\!] = \mathsf{false}$

$\mathsf{fix}X.P \equiv P\{^{\mathsf{fix}X.P}/_X\}$

Networks:

$P \equiv Q$ implies $n[\mathscr{I} \bowtie P]^{\mu}_{h} \equiv n[\mathscr{I} \bowtie Q]^{\mu}_{h}$

$M \mid \mathbf{0} \equiv M$

$M \mid N \equiv N \mid M$

$(M \mid N) \mid O \equiv M \mid (N \mid O)$

$(\nu c)\mathbf{0} \equiv \mathbf{0}$

$(\nu c)(\nu d)M \equiv (\nu d)(\nu c)M$

$(\nu c)(M \mid N) \equiv M \mid (\nu c)N$ if c not in M

Condition (iv) requires that the physical devices (sensors and actuators) accessed by the controller processes must be defined in the corresponding physical interface of the node. Last condition implies that location-dependent sensors may be used only in stationary nodes. This restriction will be commented in Section 2.3. Hereafter, we will always work with *well-formed networks*. It is easy to show that well-formedness is preserved at runtime.

Finally, we assume a number of *notational conventions*. $\prod_{i\in I} M_i$ denotes the parallel composition of all M_i, for $i \in I$. We identify $\prod_{i\in I} M_i = \mathbf{0}$ and $\prod_{i\in I} P_i = \mathsf{nil}$, if $I = \emptyset$. Sometimes we write $\prod_i M_i$ when the index set I is not relevant. We write ρ instead of the process $\rho.\mathsf{nil}$. For $k \geq 0$, we write $\sigma^k.P$ as a shorthand for $\sigma.\sigma.\ldots.\sigma.P$, where prefix σ appears k consecutive times. Finally, we write $(\nu\tilde{c})M$ as an abbreviation for $(\nu c_1)\ldots(\nu c_k)M$, for $\tilde{c} = c_1,\ldots,c_k$.

2.1 Reduction semantics

The dynamics of the calculus is given in terms of *reduction relations* over networks, as described in Table 3. As usual in process calculi, a reduction semantics [30] relies on an auxiliary standard relation, $\equiv$, called *structural congruence*, which brings the participants of a potential interaction into contiguous positions. Formally, structural congruence is defined as the congruence induced by the axioms of Table 2 up to α-conversion.

As `CaIT` is a timed calculus, with a discrete notion of time, we will distinguish between instantaneous reductions, $M \rightarrowtriangle_{\mathrm{i}} N$, and timed reductions, $M \rightarrowtriangle_{\sigma} N$. Relation $\rightarrowtriangle_{\mathrm{i}}$ denotes activities which take place within one time interval, whereas $\rightarrowtriangle_{\sigma}$ represents the passage of one time unit. Our instantaneous reductions are of two kinds: those which involve the change of the values associated to some actuator a, written $\rightarrowtriangle_{a}$, and the others, written $\rightarrowtriangle_{\tau}$. Intuitively, reductions of the form $M \rightarrowtriangle_{a} N$ denote *watchpoints* which cannot be ignored by the physical environment (in Example 2, and more extensively at the end of Section 2.3, we explain why it is important to distinguish between $\rightarrowtriangle_{\tau}$ and $\rightarrowtriangle_{a}$). Thus, we define the instantaneous reduction relation $\rightarrowtriangle_{\mathrm{i}} \overset{\mathrm{def}}{=} \rightarrowtriangle_{\tau} \cup \rightarrowtriangle_{a}$, for any actuator a. We also define $\rightarrowtriangle \overset{\mathrm{def}}{=} \rightarrowtriangle_{\tau} \cup \rightarrowtriangle_{\sigma}$.

The first seven rules in Table 3 model intra-node activities. Rule (sensread) represents the reading of the current data detected at some sensor s. Rule (pos) serves to compute the current position of a

Table 3 Reduction semantics

$$(\text{pos})\ \frac{-}{n[\mathscr{I} \bowtie @(x).P]^{\mu}_{h} \rightarrowtriangle_{\tau} n[\mathscr{I} \bowtie P\{{}^{h}\!/\!_{x}\}]^{\mu}_{h}} \qquad (\text{sensread})\ \frac{\mathscr{I}(s) = v}{n[\mathscr{I} \bowtie s?(x).P]^{\mu}_{h} \rightarrowtriangle_{\tau} n[\mathscr{I} \bowtie P\{{}^{v}\!/\!_{x}\}]^{\mu}_{h}}$$

$$(\text{actunchg})\ \frac{\mathscr{I}(a) = v}{n[\mathscr{I} \bowtie a!v.P]^{\mu}_{h} \rightarrowtriangle_{\tau} n[\mathscr{I} \bowtie P]^{\mu}_{h}} \qquad (\text{actchg})\ \frac{\mathscr{I}(a) \neq v \quad \mathscr{I}' := \mathscr{I}[a \mapsto v]}{n[\mathscr{I} \bowtie a!v.P]^{\mu}_{h} \rightarrowtriangle_{a} n[\mathscr{I}' \bowtie P]^{\mu}_{h}}$$

$$(\text{loccom})\ \frac{\text{rng}(c) = -1}{n[\mathscr{I} \bowtie \lfloor \overline{c}\langle v \rangle.P \rfloor R \mid \lfloor c(x).Q \rfloor S]^{\mu}_{h} \ \rightarrowtriangle_{\tau}\ n[\mathscr{I} \bowtie P \mid Q\{{}^{v}\!/\!_{x}\}]^{\mu}_{h}}$$

$$(\text{timestat})\ \frac{n[\mathscr{I} \bowtie \prod_i \lfloor \pi_i.P_i \rfloor Q_i \mid \prod_j \sigma.R_j]^{\mathtt{s}}_{h} \not\rightarrowtriangle_{\tau}}{n[\mathscr{I} \bowtie \prod_i \lfloor \pi_i.P_i \rfloor Q_i \mid \prod_j \sigma.R_j]^{\mathtt{s}}_{h} \rightarrowtriangle_{\sigma} n[\mathscr{I} \bowtie \prod_i Q_i \mid \prod_j R_j]^{\mathtt{s}}_{h}}$$

$$(\text{timemob})\ \frac{n[\mathscr{I} \bowtie \prod_i \lfloor \pi_i.P_i \rfloor Q_i \mid \prod_j \sigma.R_j]^{\mathtt{m}}_{h} \not\rightarrowtriangle_{\tau} \qquad \text{d}(h,k) \leq \delta}{n[\mathscr{I} \bowtie \prod_i \lfloor \pi_i.P_i \rfloor Q_i \mid \prod_j \sigma.R_j]^{\mathtt{m}}_{h} \rightarrowtriangle_{\sigma} n[\mathscr{I} \bowtie \prod_i Q_i \mid \prod_j R_j]^{\mathtt{m}}_{k}}$$

$$(\text{glbcom})\ \frac{\text{d}(h,k) \leq \text{rng}(c)}{n[\mathscr{I} \bowtie \lfloor \overline{c}\langle v \rangle.P \rfloor R]^{\mu_1}_{h} \mid m[\mathscr{J} \bowtie \lfloor c(x).Q \rfloor S]^{\mu_2}_{k} \rightarrowtriangle_{\tau} n[\mathscr{I} \bowtie P]^{\mu_1}_{h} \mid m[\mathscr{J} \bowtie Q\{{}^{v}\!/\!_{x}\}]^{\mu_2}_{k}}$$

$$(\text{parp})\ \frac{\prod_i n_i[\mathscr{I}_i \bowtie P_i]^{\mu_i}_{h_i} \rightarrowtriangle_{\omega} \prod_i n_i[\mathscr{I}'_i \bowtie P'_i]^{\mu_i}_{h_i} \quad \omega \in \{\tau, a\}}{\prod_i n_i[\mathscr{I}_i \bowtie P_i \mid Q_i]^{\mu_i}_{h_i} \rightarrowtriangle_{\omega} \prod_i n_i[\mathscr{I}'_i \bowtie P'_i \mid Q_i]^{\mu_i}_{h_i}} \qquad (\text{parn})\ \frac{M \rightarrowtriangle_{\omega} M' \quad \omega \in \{\tau, a\}}{M \mid N \rightarrowtriangle_{\omega} M' \mid N}$$

$$(\text{timepar})\ \frac{M \rightarrowtriangle_{\sigma} M' \quad N \rightarrowtriangle_{\sigma} N' \quad M \mid N \not\rightarrowtriangle_{\tau}}{M \mid N \rightarrowtriangle_{\sigma} M' \mid N'} \qquad (\text{timezero})\ \frac{-}{\mathbf{0} \rightarrowtriangle_{\sigma} \mathbf{0}}$$

$$(\text{res})\ \frac{M \rightarrowtriangle_{\omega} N \quad \omega \in \{\tau, a, \sigma\}}{(\nu c)M \rightarrowtriangle_{\omega} (\nu c)N} \qquad (\text{struct})\ \frac{M \equiv N \ N \rightarrowtriangle_{\omega} N' \ \omega \in \{\tau, a, \sigma\} \ N' \equiv M'}{M \rightarrowtriangle_{\omega} M'}$$

node. Rules (actunchg) and (actchg) implement the writing of some data v on an actuator a, distinguishing whether the value of the actuator changes or not. Rule (loccom) models intra-node communications on a local channel c ($\text{rng}(c) = -1$). Rule (timestat) models the passage of time within a stationary node. Notice that all untimed intra-node actions are considered urgent actions as they must occur before the next timed action. As an example, position detection is a time-dependent operation which cannot be delayed. Similar argument applies to sensor reading, actuator writing and channel communication. Rule (timemob) models the passage of time within a mobile node. This rule also serves to model *node mobility*. Mobile nodes can nondeterministically move from one physical location h to a (possibly different) location k, at the end of a time interval. Node mobility respects the following time discipline: in one time unit a node located at h can move to any location k such that $\text{d}(h,k) \leq \delta$, for some fixed $\delta \in \mathbb{N}$ (obviously, it is possible to have $h = k$ and $\text{d}(h,k) = 0$). For the sake of simplicity, we fix the same constant δ for all nodes of our systems. The premises of Rules (timestat) and (timemob) ensure that if a node can perform a timed reduction $\rightarrowtriangle_{\sigma}$ then the same node cannot perform an instantaneous reduction $\rightarrowtriangle_{\tau}$. Actually, due to the syntactic restrictions in the premises of both rules, that node cannot perform an instantaneous reduction $\rightarrowtriangle_{a}$ either. This is formalised in Proposition 2.

Rule (glbcom) models inter-node communication along a global channel c ($\text{rng}(c) \geq 0$). Intuitively, two different nodes can communicate via a common channel c if and only if they are within the transmission range of c. Rules (parp) and (parn) serve to propagate instantaneous reductions through parallel processes, and parallel networks, respectively. Rule (timepar) is for inter-node time synchronisation; the passage of time is allowed only if all instantaneous reductions have already fired. *Well-timedness* (Proposition 4) ensures the absence of infinite instantaneous traces which would prevent the passage of time. The remaining rules are standard.

We write $\rightarrowtriangle_{\mathrm{i}}^{k}$ as an shorthand for k consecutive reductions $\rightarrowtriangle_{\mathrm{i}}$; $\rightarrowtriangle_{\mathrm{i}}^{*}$ is the reflexive and transitive closure of $\rightarrowtriangle_{\mathrm{i}}$. Similar conventions apply to the reduction relation $\rightarrowtriangle$.

Below we report a few standard time properties which hold in our calculus: *time determinism*, *maximal progress*, *patience* and *well-timedness*. In its standard formulation, *time determinism* says that a system reaches at most one new state by executing a reduction $\rightarrowtriangle_{\sigma}$. However, by an application of Rule (timemob), our mobile nodes may change location when executing a reduction $\rightarrowtriangle_{\sigma}$, thus we have a local variant of time determinism.

Proposition 1 (Local time determinism). *If $M \rightarrowtriangle_{\sigma} M'$ and $M \rightarrowtriangle_{\sigma} M''$, then $M' \equiv \prod_{i\in I} n_i[\mathscr{I}_i \bowtie P_i]_{h_i}^{\mu_i}$ and $M'' \equiv \prod_{i\in I} n_i[\mathscr{I}_i \bowtie P_i]_{k_i}^{\mu_i}$, with $\mathrm{d}(h_i,k_i) \leq 2\delta$, for all $i \in I$.*

According to [19], the *maximal progress* property says that processes communicate as soon as a possibility of communication arises. In our calculus, we generalise this property saying that instantaneous reductions cannot be delayed.

Proposition 2 (Maximal progress). *If $M \rightarrowtriangle_{\mathrm{i}} M'$, then there is no M'' such that $M \rightarrowtriangle_{\sigma} M''$.*

On the other hand, if no instantaneous reductions are possible then time is free to pass.

Proposition 3 (Patience). *If $M \rightarrowtriangle_{\mathrm{i}} M'$ for no M', then there is N such that $M \rightarrowtriangle_{\sigma} N$.*

Finally, time passing cannot be prevented by infinite sequences of internal actions. Formally,

Proposition 4 (Well-timedness). *For any M there is a $z \in \mathbb{N}$ such that if $M \rightarrowtriangle_{\mathrm{i}}^{u} N$ then $u \leq z$.*

The proof of Proposition 4 relies on time-guardedness of recursive processes.

2.2 Contextual behavioural equivalence

In this section we provide a standard notion of contextual equivalence for our systems. Our touchstone equivalence is *reduction barbed congruence* [20, 31], a standard contextually defined process equivalence. Intuitively, two systems are reduction barbed congruent if they have the same *basic observables* in all *contexts* and under all possible *computations*.

As already pointed out in the Introduction, the definition of reduction barbed congruence relies on two crucial concepts: a *reduction semantics* to describe system computations, and the *basic observable*, or barbs, which denotes what the environment can directly observe of a system[1]. So, the question now is: What are the right observables in our calculus? Due to the cyber-physical nature of our systems we could choose to observe either channel communications (logical observation) as in standard process calculi, or the capability to diffuse messages via actuators (physical observation). Actually, it turns out that logical observation in `CaIT` can be expressed in terms of physical one (see Section 2.3 for details) while the vice versa does not hold. So, we adopt as basic observables the capability to publish messages on actuators.

Definition 2 (Barbs). *We write $M \downarrow_{a@h!v}$ if $M \equiv (\nu \tilde{g})\big(n[\mathscr{I} \bowtie P]_{h}^{\mu} \mid M'\big)$ with $\mathscr{I}(a) = v$. We write $M \Downarrow_{a@h!v}$ if $M \rightarrowtriangle^{*} M' \downarrow_{a@h!v}$.*

The reader may wonder why our barb reports the location and not the node of the actuator. We recall that actuator names are unique, so they somehow codify the name of their node. The location is then necessary because the environment is potentially aware of its position when observing an actuator: if on Monday at 6.00AM your smartphone rings to wake you up, then you may react differently depending whether you are at home or on holidays in the Bahamas!

[1] See [37] for a comparison between this approach and the original barbed congruence [31].

Definition 3. *A binary relation $\mathcal{R}$ over networks is* barb preserving *if $M \mathrel{\mathcal{R}} N$ and $M \downarrow_{a@h!v}$ implies $N \Downarrow_{a@h!v}$.*

Definition 4. *A binary relation $\mathcal{R}$ over networks is* reduction closed *if whenever $M \mathrel{\mathcal{R}} N$ the following conditions are satisfied:*

- *$M \rightarrowtriangle M'$ implies $N \rightarrowtriangle^* N'$ and $M' \mathrel{\mathcal{R}} N'$*
- *$M \rightarrowtriangle_a M'$ implies $N \rightarrowtriangle^* \rightarrowtriangle_a \rightarrowtriangle^* N'$ and $M' \mathrel{\mathcal{R}} N'$.*

Here, we require reduction closure of both $\rightarrowtriangle$ and $\rightarrowtriangle_a$, for any a. This is a *crucial design decision* in `CaIT`. (see Example 2 and Section 2.3 for details).

In order to model sensor updates made by the physical environment on a sensor s in a given location h, we define an operator $[s@h \mapsto v]$ on networks.

Definition 5. *Given a location h, a sensor s, and a value v in the domain of s, we define:*

$$\begin{aligned}
n[\mathcal{I} \bowtie P]^{\mu}_{h}[s@h \mapsto v] &\stackrel{\text{def}}{=} n[\mathcal{I}[s \mapsto v] \bowtie P]^{\mu}_{h}, \textit{ if } \mathcal{I}(s) \textit{ defined}\\
n[\mathcal{I} \bowtie P]^{\mu}_{k}[s@h \mapsto v] &\stackrel{\text{def}}{=} n[\mathcal{I} \bowtie P]^{\mu}_{k}, \textit{ if } \mathcal{I}(s) \textit{ undefined or } h \neq k\\
(M \mid N)[s@h \mapsto v] &\stackrel{\text{def}}{=} M[s@h \mapsto v] \;\mid\; N[s@h \mapsto v]\\
\big((\nu c)M\big)[s@h \mapsto v] &\stackrel{\text{def}}{=} (\nu c)\big(M[s@h \mapsto v]\big)\\
\mathbf{0}[s@h \mapsto v] &\stackrel{\text{def}}{=} \mathbf{0} \ .
\end{aligned}$$

As for barbs, the reader may wonder why when updating a sensor we use its location, also for node-dependent sensors. This is because when changing a node-dependent sensor (e.g. touching a touchscreen of a smartphone) the environment is in general aware of its position.

Definition 6. *A binary relation $\mathcal{R}$ over networks is* contextual *if $M \mathrel{\mathcal{R}} N$ implies that*

- *for all networks O, $M \mid O \;\mathcal{R}\; N \mid O$*
- *for all channels c, $(\nu c)M \;\mathcal{R}\; (\nu c)N$*
- *for all sensors s, locations h, and values v in the domain of s, $M[s@h \mapsto v] \mathrel{\mathcal{R}} N[s@h \mapsto v]$.*

The first two clauses requires closure under *logical contexts* (parallel systems), while the last clause involves *physical contexts*, which can *nondeterministically update* sensor values.

Finally, everything is in place to define our touchstone contextual behavioural equality.

Definition 7. Reduction barbed congruence*, written $\cong$, is the largest symmetric relation over networks which is reduction closed, barb preserving and contextual.*

Remark 1. *Obviously, if $M \cong N$ then M and N will be still equivalent in any setting where sensor updates are governed by specific physical laws. This is because the physical contexts that can affect sensor values, according to some physical law, are definitely fewer than those which can change sensors nondeterministically.*

We recall that the reduction relation $\rightarrowtriangle$ ignores the passage of time, and therefore the reader might suspect that our reduction barbed congruence is impervious to the precise timing of activities. We will show that this is not the case.

Example 1. *Let M and N be two networks such that $M = n[\emptyset \bowtie \sigma.\lfloor \overline{c}\langle v\rangle.\mathsf{nil} \rfloor \mathsf{nil}]^{\mathsf{s}}_{h}$ and $N = n[\emptyset \bowtie \lfloor \overline{c}\langle v\rangle.\mathsf{nil} \rfloor \mathsf{nil}]^{\mathsf{s}}_{h}$, with $\mathrm{rng}(c) = \infty$. It is easy to see that $M \rightarrowtriangle_{\sigma} N$. As the reduction relation $\rightarrowtriangle$ does not distinguish instantaneous reductions from timed ones, one may think that networks M and N are reduction barbed congruent, and that a prompt transmission along channel c is equivalent to the same transmission delayed of one time unit. However, let us consider the test $T = test[\mathcal{J} \bowtie \sigma.a!1.\lfloor c(x).a!0 \rfloor \mathsf{nil}]^{\mathsf{s}}_{l}$, with $\mathcal{J}(a) = 0$, for some* *(fresh) actuator a. Our claim is that test T can distinguish the two networks, and thus $M \not\cong N$. In fact, if $M \mid T \rightarrowtriangle\rightarrowtriangle_a O = n[\emptyset \bowtie \lfloor \overline{c}\langle v\rangle.\mathsf{nil} \rfloor \mathsf{nil}]^{\mathsf{s}}_{h} \mid \mathit{test}[\mathscr{J}' \bowtie \lfloor c(x).a!0 \rfloor \mathsf{nil}]^{\mathsf{s}}_{l}$, with $\mathscr{J}'(a) = 1$, then there is no O' such that $N \mid T \rightarrowtriangle^{*}\rightarrowtriangle_a\rightarrowtriangle^{*} O'$ with $O \cong O'$. This is because O can perform a reduction sequence $\rightarrowtriangle\rightarrowtriangle_a$ that cannot be matched by any O'.*

Behind this example there is the general principle that reduction barbed congruence is sensitive to the passage of time.

Proposition 5. *If $M \cong N$ and $M \rightarrowtriangle_{\sigma} M'$ then there is N' such that $N \rightarrowtriangle_{\tau}^{*}\rightarrowtriangle_{\sigma}\rightarrowtriangle_{\tau}^{*} N'$ and $M' \cong N'$.*

Proof. Suppose $M \rightarrowtriangle_{\sigma} M'$. Consider the test node $T = \mathit{test}[\mathscr{J} \bowtie \sigma.a!1.a!0]^{\mathsf{s}}_{k}$ such that both systems $M \mid T$ and $N \mid T$ are well-formed, and $\mathscr{J}(a) = 0$. By construction, the presence of a barb $\Downarrow_{a@k!1}$ in a derivative of one of those systems implies that exactly one timed reduction $\rightarrowtriangle_{\sigma}$ has been inferred in the derivation.

Since $M \rightarrowtriangle_{\sigma} M'$ it follows that $M \mid T \rightarrowtriangle_{\sigma}\rightarrowtriangle_a M' \mid T'$, with $T' = \mathit{test}[\mathscr{J}[a \mapsto 1] \bowtie a!0]^{\mathsf{s}}_{k}$ and $M' \mid T' \downarrow_{a@k!1}$. As $M \cong N$ and $\cong$ is contextual, the reduction sequence above must be mimicked by $N \mid T$, that is $N \mid T \rightarrowtriangle^{*}\rightarrowtriangle_a\rightarrowtriangle^{*} \hat{N}$, with $M' \mid T' \cong \hat{N}$. As a consequence, $\hat{N} \Downarrow_{a@k!1}$. This implies that exactly one timed reduction has been inferred in the reduction sequence $N \mid T \rightarrowtriangle^{*}\rightarrowtriangle_a\rightarrowtriangle^{*} \hat{N}$. As $M \mid T$ and $N \mid T$ are well-formed networks, the actuator a can appear neither in M nor in N. So, the above reduction sequence can be decomposed as follows:

$$N \mid T \rightarrowtriangle^{*} N' \mid T \rightarrowtriangle_a N' \mid T' \rightarrowtriangle^{*} N'' \mid T' = \hat{N}$$

with $N \rightarrowtriangle_{\tau}^{*}\rightarrowtriangle_{\sigma}\rightarrowtriangle_{\tau}^{*} N''$. From $M' \mid T' \cong N'' \mid T'$ it is easy to derive $M' \cong N''$ (for details see Lemma 2 in Section 5). □

Now, we provide some insights into the design decision of having two different reduction relations $\rightarrowtriangle_{\tau}$ and $\rightarrowtriangle_a$.

Example 2. *Let $M = n[\mathscr{I} \bowtie a!1 \mid a!0.a!1]^{\mu}_{h}$ and $N = n[\mathscr{I} \bowtie a!1.a!0.a!1]^{\mu}_{h}$, with $\mathscr{I}(a) = 0$ and undefined otherwise. Then, within one time unit, M may display on the actuator a either the sequence of values* 01 *or the sequence* 0101, *while N can only display the sequence* 0101. *As a consequence, from the point of view of the physical environment, the observable behaviours of M and N are clearly different. In the following we show how $\cong$ can observe that difference. We recall that the relation $\cong$ is reduction closed. Now, if $M \rightarrowtriangle_{\tau}\rightarrowtriangle_a M' = n[\mathscr{J} \bowtie a!1]^{\mu}_{h}$, with $\mathscr{J}(a) = 1$, the only possible reply of N respecting reduction closure is $N \rightarrowtriangle^{*}\rightarrowtriangle_a N' = n[\mathscr{J} \bowtie a!0.a!1]^{\mu}_{h}$. However, it is evident that $M' \not\cong N'$ because N' can turn the actuator a to* 0 *while M' cannot. Thus, $M \not\cong N$.*

Had we merged the relation $\rightarrowtriangle_a$ with $\rightarrowtriangle_{\tau}$ then we would have $M \cong N$ because the capability to observe messages on actuators, given by the barb, would not be enough to observe changes on actuators within one time interval.

2.3 Design choices

In this section we provide some insights into the design choices which have be followed in the definition of `CaIT`.

`CaIT` is a *value-passing* rather than a *name-passing* calculus, à la π-calculus [37]; the theory of `CaIT` can be easily adapted to deal with the transmission of channel names at the price of adding the standard burden of scope-extrusion of names. Furthermore, as both actuators and sensors can only be managed inside their nodes, it would make little sense to transmit their names along channels. For simplicity, in `CaIT` we adopt a *point-to-point communication* via communication channels. Broadcast communications could be easily introduced along the lines of Merro's CMN [26], without affecting the main theoretical results.

CaIT is a timed process calculus with a discrete notion of time. The time model we adopt in CaIT is known as the *fictitious clock approach* (see e.g. [19]): a global clock is supposed to be updated whenever all nodes agree on this, by globally synchronising on a special timing action σ. Thus, time synchronisation relies on some clock synchronisation protocol for mobile wireless systems [40]. However, our notion of time interval is different from that adopted in synchronous languages [5, 1, 8] where the environment injects events at the beginning a time interval and collect them at the end. In the synchronous approach, events happening during a time interval are not ordered while in our calculus we want to maintain the causality among actions, typical of process calculi.

We already said that IoT systems are essentially *cyber-physical systems* [38]. In cyber-physical systems, sensor changes are usually modelled either using continuous models, such as differential equations, or through discrete models, such as difference equations [2]. However, in this paper we aim at providing a behavioural semantics for IoT applications from the point of the view of the end user. And the end user cannot directly observe changes on the sensors of an IoT application: she can only observe the effects of those changes via actuators and communication channels. Thus, in CaIT we do not represent sensor changes via specific models, but we rather abstract on them by supporting *nondeterministic sensor updates* (see Definition 5 and Definition 6). Actually, as pointed out in Remark 1, behavioural equalities derived in our setting remains valid when adopting any specific model for sensor updates.

Another design decision in our language regards the possibility to change the value associated to sensors and actuators more than once within the same time interval. At first sight this choice may appear weird as certain actuators are physical devices that may require some time to turn on. On the other hand, other actuators, such as lights or displays, may have very quick reactions. A similar argument applies to sensors. In this respect our calculus does not enforce a synchronisation of physical events as for logical signals in synchronous languages. In fact, actuator changes are under nodes' control: the process running within a node decides when changing the value exposed on an actuator of that node. Thus, if the actuator of a node models a slow device then it is under the responsibility of the process running at that node to change the actuator with a proper delay. Similarly, sensors should be read only when this makes sense. For instance, a temperature sensor should be read only when the temperature is known to be stable.

Let us now discuss on node mobility. The reader may wonder why CaIT does not provide a process for node mobility, as in Mobile Ambients [9]. Notice that, unlike Mobile Ambients, our nodes do not represent mobile computations within an Internet domain. Instead, they represent smart devices which do not decide where to move to: an external agent moves them. We also decided to allow node mobility only at the end of time intervals. This is because both intra-node and inter-node logical operations, such as channel communications, can be considered significantly faster than physical movements of devices. For instance, consider a transmitter that moves at 20 m/s and that transmits a 2000-byte frame over a channel having a 2 megabit/s bandwidth. The actual transmission would take about 0.008 s; during that time, the transmitter moves only about 16 cm away. In other words, we can assume that the nodes are stationary when transmitting and receiving, and may change their location only while they are idle. However, to avoid uncontrolled movements of nodes we decided to fix for all of them the same bound δ, representing the maximum distance a node can travel within one time unit. There would not be problems in allowing different δ for different nodes. Finally, for the sake of simplicity, in the last constraint of Definition 1 we impose that location-dependent sensors can only occur in stationary nodes. This allows us to have a local, rather than a global, representation of those sensors. Notice that mobile location-dependent sensors would

[2] Difference equations relate to differential equations as discrete math relate to continuous math.

have the same technical challenges of *mobile wireless sensor networks* [42].

Another issue is about a proper representation of network topology. A tree-structure topology, as in Mobile Ambients, would be desirable to impose that a device cannot be in two mutually exclusive places at the same time. This desirable property cannot be expressed in [22], where links between nodes can be added and removed nondeterministically. However, a tree-structured topology would imply an higher-order bisimulation (for details see [29]); while in the current paper we look for a simple (first-order) bisimulation proof-technique which could be easily mechanised.

Finally, we would like to explain our choice about barbs. As already said in the previous section there are other possible definitions of barb. For instance, one could choose to observe the capability to transmit along a channel c, by defining $M \downarrow_{\overline{c}@h}$ if $M \equiv (\nu\tilde{g})\big(n[\mathscr{I} \bowtie \lfloor\overline{c}\langle v\rangle.P\rfloor P' \mid Q]^{\mu}_{k} \mid M'\big)$, with $c \notin \tilde{g}$ and $\mathrm{d}(h,k) \leq \mathrm{rng}(c)$. However, if you consider the system $S = (\nu c)(M \mid m[\mathscr{J} \bowtie \lfloor c(x).a!1\rfloor \mathsf{nil}]^{\mu}_{h})$, with $\mathscr{J}(a) = 0$, for some appropriate m, then it is easy to show that $M \downarrow_{\overline{c}@h}$ if and only if $S \rightarrowtriangle\rightarrowtriangle_{a} S' \downarrow_{a@h!1}$. Thus, the barb on channels can always be reformulated in terms of our barb. The vice versa is not possible. The reader may also wonder whether it is possible to turn the reduction $\rightarrowtriangle_{a}$ into $\rightarrowtriangle_{\tau}$ by introducing, at the same time, some special barb which would be capable to observe actuators changes. For instance, something like $M \downarrow_{a@h!v.w}$ if $M \equiv (\nu\tilde{g})\big(n[\mathscr{I} \bowtie a!w.P \mid Q]^{\mu}_{h} \mid M'\big)$, with $\mathscr{I}(a) = v$ and $v \neq w$. It should be easy to see that this extra barb would not help in distinguishing the terms proposed in Example 2. Actually, here there is something deeper that needs to be spelled out. In process calculi, the term β of a barb $\downarrow_{\beta}$ is a concise encoding of a context C_{β} expressible in the calculus and capable to observe the barb $\downarrow_{\beta}$. However, our barb $\downarrow_{a@h!v}$ does not have such a corresponding *physical context* in our language. For instance, in `CaIT` we do not represent the "eyes of a person" looking at the values appearing to some display. Technically speaking, we don't have terms of the form $a?(x).P$ that could be used by the physical environment to read values on the actuator a. This is because such terms would not be part of an IoT system. The lack of this physical context, together with the persistent nature of actuators' state, explains why our barb $\downarrow_{a@h!v}$ must work together with the reduction relation $\rightarrowtriangle_{a}$ to provide the desired distinguishing power of $\cong$. On the other hand, the decision of not including $\rightarrowtriangle_{a}$ as part of $\rightarrowtriangle$ gives to $\cong$ enough distinguishing power to observe strong preservation of barbs.

Proposition 6. *If $M \cong N$ and $M \downarrow_{a@h!v}$ then $N \downarrow_{a@h!v}$.*

Proof. We recall that $\rightarrowtriangle \stackrel{\text{def}}{=} \rightarrowtriangle_{\tau} \cup \rightarrowtriangle_{\sigma}$. Suppose $M \downarrow_{a@h!v}$. As $\cong$ is barb preserving it follows that $N \Downarrow_{a@h!v}$, namely, $N \rightarrowtriangle^{*} N' \downarrow_{a@h!v}$, for some N'. However, both reduction relations $\rightarrowtriangle_{\tau}$ and $\rightarrowtriangle_{\sigma}$ do not modify actuator values. As a consequence, this holds also for $\rightarrowtriangle$. Thus, it follows that $N \downarrow_{a@h!v}$. □

3 Case study: a smart home

In this section, we model the simple smart home discussed in the Introduction, and represented in Figure 1. The house consists of an entrance and a lounge, separated by a patio. It spans over 4 contiguous physical locations $loci$, for $i = [1..4]$, such that $\mathrm{d}(loci, locj) =\mid i - j \mid$. The entrance is in $loc1$, the patio spans from $loc2$ to $loc3$, and the lounge is in $loc4$. The house can only be accessed via its entrance. Entrance and lounge have their own lights (actuators) which are governed by different light manager processes, *LightMng*. The boiler is in the patio and is governed by a boiler manager process, *BoilerMng*. This process senses the local temperature (via a sensor) and decides whether the boiler should be turned on/off, setting a proper actuator to signal the state of the boiler. The smartphone executes two concurrent processes: *BoilerCtrl* and *LightCtr*. The first one reads user's commands for the boiler, submitted via the phone touchscreen (a sensor), and forward them to the process *BoilerMng*, via an Internet channel. Whereas, the

Table 4 A smart home in `CaIT`

$$
\begin{aligned}
\mathit{Sys} &\stackrel{\text{def}}{=} \mathit{Phone} \;\big|\; \mathit{Home}\\
\mathit{Phone} &\stackrel{\text{def}}{=} n_P[\mathscr{I}_P \bowtie \mathit{BoilerCtrl} \mid \mathit{LightCtrl}]^{\mathtt{m}}_{\mathit{out}}\\
\mathit{Home} &\stackrel{\text{def}}{=} \mathit{LM}_1 \;\big|\; \mathit{LM}_2 \;\big|\; \mathit{BM}\\
\mathit{LM}_1 &\stackrel{\text{def}}{=} n_1[\mathscr{I}_1 \bowtie \mathit{LightMng}_{\mathit{1}}]^{\mathtt{s}}_{\mathit{loc}1}\\
\mathit{LM}_2 &\stackrel{\text{def}}{=} n_2[\mathscr{I}_2 \bowtie \mathit{LightMng}_{2}]^{\mathtt{s}}_{\mathit{loc}4}\\
\mathit{BM} &\stackrel{\text{def}}{=} n_B[\mathscr{I}_B \bowtie \mathit{BoilerMng}]^{\mathtt{s}}_{\mathit{loc}2}\\
\mathit{BoilerCtrl} &\stackrel{\text{def}}{=} \mathsf{fix}X.\mathit{mode}?(z).\lfloor \overline{b}\langle z\rangle.\sigma.X\rfloor X\\
\mathit{LightCtrl} &\stackrel{\text{def}}{=} \textstyle\prod_{j=1}^{2} \mathsf{fix}X.\lfloor \overline{c_j}\langle \mathsf{on}\rangle.\sigma.X\rfloor X\\
\mathit{LightMng}_j &\stackrel{\text{def}}{=} \mathsf{fix}X.\lfloor c_j(x).\mathit{light}_j!\mathsf{on}.\sigma.X\rfloor \mathit{light}_j!\mathsf{off}.X \quad \text{for } j \in \{1,2\}\\
\mathit{BoilerMng} &\stackrel{\text{def}}{=} \mathsf{fix}X.\lfloor b(x).[x = \mathsf{man}]\,\mathit{boiler}!\mathsf{on}.\sigma.\mathit{BoilerManual};\mathit{TempCtrl}\rfloor \mathit{TempCtrl}\\
\mathit{BoilerManual} &\stackrel{\text{def}}{=} \mathsf{fix}Y.b(y).[y = \mathsf{auto}]X;\sigma.Y\\
\mathit{TempCtrl} &\stackrel{\text{def}}{=} \mathit{temp}?(t).[t < \Theta]\,\mathit{boiler}!\mathsf{on}.\sigma.X;\mathit{boiler}!\mathsf{off}.\sigma.X
\end{aligned}
$$

process *LightCtrl* interacts with the processes *LightMng*, via short-range wireless channels (e.g. Bluetooth, infrared, etc), to automatically turn on lights when the smartphone physically enters either the entrance or the lounge.

Table 4 provides a detailed formalisation of our smart home in `CaIT`. The whole system, *Sys*, is given by the parallel composition of the smartphone *Phone* (a mobile device) and the smart home *Home* (a stationary entity). The smartphone is represented as a mobile node, with $\delta = 1$, initially placed outside the house: $\mathit{out} \neq \mathit{loc}j$, for $j \in [1..4]$. As the phone can only access the house from its entrance, and $\delta = 1$, we have $\mathrm{d}(l, \mathit{loc}i) \geq i$, for any $l \notin \{\mathit{loc}1, \mathit{loc}2, \mathit{loc}3, \mathit{loc}4\}$ and $i \in [1..4]$. Its interface $\mathscr{I}_P$ contains only one sensor, called *mode*, representing the touchscreen to control the boiler. This is a node-dependent sensor. The process *BoilerCtrl* reads sensor *mode* and forwards its value to the boiler manager in the patio, *BoilerMng*, via the Internet channel b ($\mathrm{rng}(b) = \infty$). The domain of the sensor *mode* is the set $\{\mathsf{man}, \mathsf{auto}\}$, where man stands for manual and auto for automatic; initially, $\mathscr{I}_P(\mathit{mode}) = \mathsf{auto}$.

In *Phone* there is a second process, called *LightCtrl*, which allows the smartphone to switch on lights *only when* getting in touch with the light managers installed in the rooms. Here channels c_1 and c_2 serve to control the lights of entrance and lounge, respectively; these are short-range channels: $\mathrm{rng}(c_1) = \mathrm{rng}(c_2) = 0$.

The smart home *Home* consists of three stationary nodes: LM_1, LM_2 and *BM*.

The light managers processes $\mathit{LightMng}_{\mathit{1}}$ and $\mathit{LightMng}_2$, are placed in LM_1 and LM_2, respectively. They manage the corresponding lights via the actuators light_j, for $j \in \{1,2\}$. The domain of these actuators is $\{\mathsf{on}, \mathsf{off}\}$; initially, $\mathscr{I}_j(\mathit{light}_j) = \mathsf{off}$, for $j \in \{1,2\}$.

The boiler manager process *BoilerMng* is placed in *BM* (node n_B). Here, the physical interface $\mathscr{I}_B$ contains a sensor named *temp* and an actuator called *boiler*; *temp* is a location-dependent temperature sensor, whose domain is $\mathbb{N}$, and *boiler* is an actuator to display boiler functionality, whose domain is $\{\mathsf{on}, \mathsf{off}\}$. The boiler manager can work either in automatic or in manual mode. In automatic mode, sensor *temp* is periodically checked: if the temperature is under a threshold Θ then the boiler will be switched on, otherwise it will be switched off. Conversely, in manual mode, the boiler is always switched on. Initially, the boiler is in automatic mode, $\mathscr{I}_B(\mathit{temp}) = \Theta$, and $\mathscr{I}_B(\mathit{boiler}) = \mathsf{off}$.

Our system *Sys* enjoys a number of desirable *run-time properties*. For instance, if the boiler is in

Table 5 Smart home in `CaIT` with a position based light management

$\overline{Sys}$	$\stackrel{\text{def}}{=}$	$\overline{Phone} \; \big\vert \; \overline{Home}$
$\overline{Phone}$	$\stackrel{\text{def}}{=}$	$n_P[\mathscr{I}_P \bowtie BoilerCtrl \mid \overline{LightCtrl}]^{\mathtt{m}}_{out}$
$\overline{Home}$	$\stackrel{\text{def}}{=}$	$Home \; \big\vert \; \overline{CLM}$
$\overline{CLM}$	$\stackrel{\text{def}}{=}$	$n_C[\emptyset \bowtie \overline{CLightMng}]^{\mathtt{s}}_{loc3}$
$\overline{LightCtrl}$	$\stackrel{\text{def}}{=}$	$\mathsf{fix}X.@(x).\lfloor \overline{g}\langle x\rangle.\sigma.X \rfloor X$
$\overline{CLightMng}$	$\stackrel{\text{def}}{=}$	$\mathsf{fix}X.\lfloor g(y).[y = loc1]\lfloor \overline{c_1}\langle \mathsf{on}\rangle.\sigma.X\rfloor X;[y = loc4]\lfloor \overline{c_2}\langle \mathsf{on}\rangle.\sigma.X\rfloor X;\sigma.X\rfloor X$

manual mode or its temperature is under the threshold Θ then the boiler will get switched on, within one time unit. Conversely, if the boiler is in automatic mode and its temperature is higher than or equal to the threshold Θ, then the boiler will get switched off within one time unit. In general, similar properties cannot be expressed in untimed calculi. Finally, our last property states the phone cannot act on the lights of the two rooms at the same time, manifesting a kind of "ubiquity".

For the sake of simplicity, in the following proposition we omit location names both in barbs and in sensor updates, writing $\downarrow_{a!v}$ instead of $\downarrow_{a@h!v}$, and $[s \mapsto v]$ instead of $[s@h \mapsto v]$. The system Sys' denotes an arbitrary (stable) derivative of Sys.

Proposition 7. *Let Sys $(\rightarrowtriangle_{\mathrm{i}}^{*}\rightarrowtriangle_{\sigma})^{*}$ Sys', for some Sys'.*

- *If $Sys'[mode{\mapsto}\mathsf{man}] \rightarrowtriangle_{\mathrm{i}}^{*} Sys'' \rightarrowtriangle_{\sigma}$ then $Sys'' \downarrow_{boiler!\mathsf{on}}$*
- *If $Sys'[temp \mapsto t] \rightarrowtriangle_{\mathrm{i}}^{*} Sys'' \rightarrowtriangle_{\sigma}$, with $t < \Theta$, then $Sys'' \downarrow_{boiler!\mathsf{on}}$*
- *If $Sys'[temp \mapsto t]\rightarrowtriangle_{\mathrm{i}}^{*}Sys'' \rightarrowtriangle_{\sigma}$, with $t \geq \Theta$, then $Sys'' \downarrow_{boiler!\mathsf{off}}$*
- *If $Sys' \rightarrowtriangle_{\mathrm{i}}^{*} Sys'' \downarrow_{light_1!\mathsf{on}}$ then $Sys'' \downarrow_{light_2!\mathsf{off}}$, and vice versa.*

The proof of Proposition 7 can be found in the Appendix.

Finally, we propose a variant of our system, where lights functionality depends on the position of the smartphone. Intuitively, the smartphone detects is current GPS position, via the process $@(x).P$, and then sends it to a centralised light manager process of the house, via an Internet channel g. We implement that by adding a module $\overline{CLM}$ inside the patio, at location $loc3$, running a process $\overline{CLightMng}$. This process will interact with the local light managers $LightMng_1$ and $LightMng_2$ to switch on/off lights, depending on the GPS position received from the smartphone. The communication between centralised and local light managers will use the two short-range channels c_1 and c_2, with slightly different transmission ranges: $\mathrm{rng}(c_1) = 2$ and $\mathrm{rng}(c_2) = 1$. In Table 5 we provide the formalisation fo this new variant where new components (with respect to those of Table 4) have been overlined.

Proposition 7 holds for system $\overline{Sys}$ as well. Actually, the two systems are closely related.

Proposition 8. *For $\delta = 1$, $(\nu\tilde{c})Sys \cong (\nu\tilde{c})(\nu g)\overline{Sys}$.*

The bisimulation proof-technique developed in the remainder of the paper will be very useful to prove such kind of non-trivial system equalities (see Proposition 10 and Theorem 4).

We end this section with a comment. While reading this case study the reader should have realised that our reduction semantics does not model sensor updates. This is because sensor changes depend on the physical environment, while a reduction semantics models the evolution of a system in isolation. Interactions with the environment will be treated in the *extensional semantics* defined in the next section.

Table 6 Intensional semantics for processes

(SndP) $\dfrac{-}{\lfloor \bar{c}\langle v\rangle.P\rfloor Q \xrightarrow{\bar{c}v} P}$	(RcvP) $\dfrac{-}{\lfloor c(x).P\rfloor Q \xrightarrow{cv} P\{^{v}/_{x}\}}$
(PosP) $\dfrac{-}{@(x).P \xrightarrow{@h} P\{^{h}/_{x}\}}$	(Com) $\dfrac{P \xrightarrow{\bar{c}v} P' \quad Q \xrightarrow{cv} Q' \quad \mathrm{rng}(c) = -1}{P \mid Q \xrightarrow{\tau} P' \mid Q'}$
(Sensor) $\dfrac{-}{s?(x).P \xrightarrow{s?v} P\{^{v}/_{x}\}}$	(Actuator) $\dfrac{-}{a!v.P \xrightarrow{a!v} P}$
(ParP) $\dfrac{P \xrightarrow{\lambda} P' \quad \lambda \neq \sigma}{P \mid Q \xrightarrow{\lambda} P' \mid Q}$	(Fix) $\dfrac{P\{^{\mathsf{fix}X.P}/_{X}\} \xrightarrow{\lambda} Q}{\mathsf{fix}X.P \xrightarrow{\lambda} Q}$
(TimeNil) $\dfrac{-}{\mathsf{nil} \xrightarrow{\sigma} \mathsf{nil}}$	(Delay) $\dfrac{-}{\sigma.P \xrightarrow{\sigma} P}$
(Timeout) $\dfrac{-}{\lfloor \pi.P\rfloor Q \xrightarrow{\sigma} Q}$	(TimeParP) $\dfrac{P \xrightarrow{\sigma} P' \quad Q \xrightarrow{\sigma} Q' \quad P \mid Q \not\xrightarrow{\tau}}{P \mid Q \xrightarrow{\sigma} P' \mid Q'}$

4 Labelled transition semantics

In this section we provide two labelled semantic models, in the SOS style of Plotkin [35]: the *intensional semantics* and the *extensional semantics*. The adjective intensional is used to stress the fact that the actions of that semantics correspond to those activities which can be performed by a system in isolation, without any interaction with the external environment. Whereas, the extensional semantics focuses on those activities which require a contribution of the environment.

4.1 Intensional semantics

Since our syntax distinguishes between networks and processes, we have two different kinds of transitions:

- $P \xrightarrow{\lambda} Q$, with $\lambda \in \{\sigma, \tau, \bar{c}v, cv, @h, s?v, a!v\}$, for *process transitions*
- $M \xrightarrow{\nu} N$, with $\nu \in \{\sigma, \tau, a, \bar{c}v@h, cv@h\}$, for *network transitions*.

In Table 6 we report standard transition rules for processes, very much in the style of [19]. Rules (SndP), (RcvP) and (Com) model communications along channel c. Rule (PosP) is for extracting the physical position of the embedding node. Rules (Sensor) and (Actuator) serve to read sensors, and to write on actuators, respectively. Rules (ParP) and (Fix) are straightforward. The remaining rules allow us the derive the timed action σ. In Rule (Delay) a timed prefix is consumed. Rule (Timeout) models timeouts when channel communication is not possible in the current time interval. Rule (TimeParP) is for time synchronisation of parallel processes. The symmetric counterparts of Rules (ParP) and (Com) are omitted. We recall that we assume $[b]P;Q = P$ if $[\![b]\!] = \mathsf{true}$, and $[b]P;Q = Q$ if $[\![b]\!] = \mathsf{false}$.

In Table 7 we report the transition rules for networks. Rule (Pos) extracts the position of a node. Rule (SensRead) models the reading of a value from a sensor of the enclosing node. Rules (ActUnChg) and (ActChg) describes the writing of a value v on an actuator a of the node, distinguishing whether the value of the actuator is changed or not. Rule (LocCom) models intra-node communications. Rule (TimeStat) models the passage of time for a stationary node. Rule (TimeMob) models both time passing and node mobility

Table 7 Intensional semantics for networks

$$(\text{Pos})\ \frac{P \xrightarrow{@h} P'}{n[\mathscr{I}\bowtie P]^{\mu}_{h} \xrightarrow{\tau} n[\mathscr{I}\bowtie P']^{\mu}_{h}} \qquad (\text{SensRead})\ \frac{\mathscr{I}(s)=v \quad P \xrightarrow{s?v} P'}{n[\mathscr{I}\bowtie P]^{\mu}_{h} \xrightarrow{\tau} n[\mathscr{I}\bowtie P']^{\mu}_{h}}$$

$$(\text{ActUnChg})\ \frac{\mathscr{I}(a)=v \quad P \xrightarrow{a!v} P'}{n[\mathscr{I}\bowtie P]^{\mu}_{h} \xrightarrow{\tau} n[\mathscr{I}\bowtie P']^{\mu}_{h}} \qquad (\text{LocCom})\ \frac{P \xrightarrow{\tau} P'}{n[\mathscr{I}\bowtie P]^{\mu}_{h} \xrightarrow{\tau} n[\mathscr{I}\bowtie P']^{\mu}_{h}}$$

$$(\text{ActChg})\ \frac{\mathscr{I}(a)\neq v \quad P \xrightarrow{a!v} P' \quad \mathscr{I}' := \mathscr{I}[a\mapsto v]}{n[\mathscr{I}\bowtie P]^{\mu}_{h} \xrightarrow{a} n[\mathscr{I}'\bowtie P']^{\mu}_{h}}$$

$$(\text{TimeStat})\ \frac{P \xrightarrow{\sigma} P' \ n[\mathscr{I}\bowtie P]^{\mathtt{s}}_{h} \not\xrightarrow{\tau}}{n[\mathscr{I}\bowtie P]^{\mathtt{s}}_{h} \xrightarrow{\sigma} n[\mathscr{I}\bowtie P']^{\mathtt{s}}_{h}} \qquad (\text{TimeMob})\ \frac{P \xrightarrow{\sigma} P' \ n[\mathscr{I}\bowtie P]^{\mathtt{m}}_{h} \not\xrightarrow{\tau} \ \mathsf{d}(h,k)\leq\delta}{n[\mathscr{I}\bowtie P]^{\mathtt{m}}_{h} \xrightarrow{\sigma} n[\mathscr{I}\bowtie P']^{\mathtt{m}}_{k}}$$

$$(\text{Snd})\ \frac{P \xrightarrow{\bar{c}v} P' \quad \mathrm{rng}(c)\geq 0}{n[\mathscr{I}\bowtie P]^{\mu}_{h} \xrightarrow{\bar{c}v@h} n[\mathscr{I}\bowtie P']^{\mu}_{h}} \qquad (\text{Rcv})\ \frac{P \xrightarrow{cv} P' \quad \mathrm{rng}(c)\geq 0}{n[\mathscr{I}\bowtie P]^{\mu}_{h} \xrightarrow{cv@h} n[\mathscr{I}\bowtie P']^{\mu}_{h}}$$

$$(\text{GlbCom})\ \frac{M \xrightarrow{\bar{c}v@k} M' \quad N \xrightarrow{cv@h} N' \quad \mathsf{d}(h,k)\leq \mathrm{rng}(c)}{M \mid N \xrightarrow{\tau} M' \mid N'}$$

$$(\text{ParN})\ \frac{M \xrightarrow{\nu} M' \quad \nu\neq\sigma}{M \mid N \xrightarrow{\nu} M' \mid N} \qquad (\text{TimePar})\ \frac{M \xrightarrow{\sigma} M' \quad N \xrightarrow{\sigma} N' \quad M \mid N \not\xrightarrow{\tau}}{M \mid N \xrightarrow{\sigma} M' \mid N'}$$

$$(\text{TimeZero})\ \frac{-}{\mathbf{0} \xrightarrow{\sigma} \mathbf{0}} \qquad (\text{Res})\ \frac{M \xrightarrow{\nu} N \quad \nu\notin\{\bar{c}v@h, cv@h\}}{(\nu c)M \xrightarrow{\nu} (\nu c)N}$$

Table 8 Extensional semantics: additional rules

$$(\text{SndObs})\ \frac{M \xrightarrow{\bar{c}v@h} M' \quad \mathsf{d}(h,k)\leq\mathrm{rng}(c)}{M \xrightarrow{\bar{c}v\triangleright k} M'} \qquad (\text{RcvObs})\ \frac{M \xrightarrow{cv@h} M' \quad \mathsf{d}(k,h)\leq\mathrm{rng}(c)}{M \xrightarrow{cv\triangleright k} M'}$$

$$(\text{SensEnv})\ \frac{v \text{ in the domain of } s}{M \xrightarrow{s@h?v} M[s@h\mapsto v]} \qquad (\text{ActEnv})\ \frac{M \downarrow_{a@h!v}}{M \xrightarrow{a@h!v} M}$$

at the end of a time interval. Rules (Snd) and (Rcv) represent transmission and reception along a global channel. Rule (GlbCom) models inter-node communications. The remaining rules are straightforward. The symmetric counterparts of Rules (ParN) and (GlobCom) are omitted.

As expected, the reduction semantics and the labelled intensional semantics coincide.

Theorem 1 (Harmony theorem)**.** *Let $\omega\in\{\tau,a,\sigma\}$:*

- $M \xrightarrow{\omega} M'$ *implies* $M \mathrel{-\!\!\triangleright}_{\omega} M'$
- $M \mathrel{-\!\!\triangleright}_{\omega} M'$ *implies* $M \xrightarrow{\omega} M''$*, for some* M'' *such that* $M'\equiv M''$.

4.2 Extensional semantics

Here we redesign our LTS to focus on the interactions of our systems with the external environment. As the environment has a *logical part* (the parallel nodes) and a *physical part* (the physical world) our extensional semantics distinguishes two different kinds of transitions:

- $M \xrightarrow{\alpha} N$, *logical transitions*, for $\alpha \in \{\tau, \sigma, a, \overline{c}v \triangleright k, cv \triangleright k\}$, to denote the interaction with the *logical environment*; here, actuator changes, τ- and σ-actions are inherited from the intensional semantics, so we don't provide inference rules for them;
- $M \xrightarrow{\alpha} N$, *physical transitions*, for $\alpha \in \{s@h?v, a@h!v\}$, to denote the interaction with the *physical world*, via sensors and actuators.

In Table 8 the extensional actions deriving from rules (SndObs) and (RcvObs) mention the location k of the logical environment which can *observe* the communication occurring at channel c. Rules (SensEnv) and (ActEnv) model the interaction of a system M with the physical environment. In particular, the environment can *nondeterministically update* the current value of a (location-dependent or node-dependent) sensor s with a value v, and can read the value v appearing on an actuator a at h. As already discussed in Section 2.2 the environment is potentially aware of its position when performing these actions.

Note that our LTSs are *image finite*. They are also *finitely branching*, and hence *mechanisable*, under the obvious assumption of finiteness of all domains of admissible values, and the set of physical locations.

5 Coinductive characterisation

Based on our extensional semantics, we are ready to define a notion of weak bisimilarity which will be showed to be both sound and complete with respect to our contextual equivalence.

We adopt a standard notation for weak transitions. We denote with $\Longrightarrow$ the reflexive and transitive closure of τ-actions, namely $(\xrightarrow{\tau})^*$, whereas $\xRightarrow{\alpha}$ means $\Longrightarrow \xrightarrow{\alpha} \Longrightarrow$, and finally $\xRightarrow{\hat{\alpha}}$ denotes $\Longrightarrow$ if $\alpha = \tau$ and $\xRightarrow{\alpha}$ otherwise.

Definition 8 (Bisimulation)**.** *A binary symmetric relation $\mathscr{R}$ over networks is a* bisimulation *if $M \mathrel{\mathscr{R}} N$ and $M \xrightarrow{\alpha} M'$ imply there exists N' such that $N \xRightarrow{\hat{\alpha}} N'$ and $M' \mathrel{\mathscr{R}} N'$. We say that M and N are* bisimilar*, written $M \approx N$, if $M \mathrel{\mathscr{R}} N$ for some bisimulation $\mathscr{R}$.*

A crucial result is that our bisimilarity is a congruence. For that we need a technical lemma on the operator of Definition 10 which returns an upper bound to the number of consecutive instantaneous reductions that a network may perform.

Lemma 1. *For any network M, sensor s, location h and value v in the domain of s, it follows that* $\mathrm{redi}(M[s@h \mapsto v]) = \mathrm{redi}(M)$.

Theorem 2. *The relation $\approx$ is contextual.*

Proof. We have to show that $\approx$ is preserved by parallel composition, channel restriction, and sensor updates. The most difficult part is to prove that $M \approx N$ entails $M[s@h \mapsto v] \approx N[s@h \mapsto v]$, for all sensors s, locations h, and values v in the domain of s. In fact, a standard approach to this proof, consisting in trying to show that the relation $\{\big(M[s@h \mapsto v], N[s@h \mapsto v]\big) : M \approx N\}$ is a bisimulation, is not affordable. In fact, in general, if $M \xrightarrow{\tau} M'$ then we do not necessarily have $M[s@h \mapsto v] \xrightarrow{\tau} M'[s@h \mapsto v]$. This is because sensor updates may have an influence on the evolution of M.

We assume a function redi() (see Definition 10 in the Appendix) which returns an upper-bound to the number of instantaneous reductions of a system. Let $\succ$ be the well-founded relation over pairs of networks such that $(M,N) \succ (M',N')$ if and only if (i) $M \approx N$; (ii) $M' \approx N'$; (iii) $\mathrm{redi}(M) + \mathrm{redi}(N) > \mathrm{redi}(M') + \mathrm{redi}(N')$. Note that $\succ$ is trivially irreflexive. Moreover, $\mathrm{redi}(M)$ always returns a finite and positive integer, for any M (see Lemma 8 in the Appendix). Thus, the relation $\succ$ does not have infinite descending chains and it is a well-founded relation.

The proof is by *well-founded induction* on the definition of $\succ$.

Base case. Let M and N be such that $M \approx N$ and $\mathrm{redi}(M) + \mathrm{redi}(N) = 0$. By Definition 10 and by inspection of the reduction semantics in Table 3, $\mathrm{redi}(N) = 0$ entails $N \not\rightarrowtriangle_{\mathrm{i}}$. In particular, we have $N \not\rightarrowtriangle_{\tau}$. By Theorem 1 it follows that $N \not\xrightarrow{\tau}$. By an application of rule (SensEnv) we derive $M \xrightarrow{s@h?v} M[s@h \mapsto v]$. As $M \approx N$ there are N_1, N_2 and N' such that $N \Rightarrow N_1 \xrightarrow{s@h?v} N_1[s@h \mapsto v] = N_2 \Rightarrow N'$ with $M[s@h \mapsto v] \approx N'$. However, as $N \not\xrightarrow{\tau}$ it follows that $N = N_1$. By Lemma 1, $N_1 \not\xrightarrow{\tau}$ entails $N_1[s@h \mapsto v] \not\xrightarrow{\tau}$. This is enough to derive that $N' = N[s@h \mapsto v]$. And hence $M[s@h \mapsto v] \approx N[s@h \mapsto v]$.

Inductive Case. Let $M \approx N$. Without loss of generality we can assume $\mathrm{redi}(M) \geq \mathrm{redi}(N)$. Let $M \xrightarrow{s@h?v} M[s@h \mapsto v]$. As $M \approx N$ there is N' such that $N \xRightarrow{s@h?v} N'$ and $M[s@h \mapsto v] \approx N'$.

Now, if the number of τ-actions contained in the weak transition $N \xRightarrow{s@h?v} N'$ is 0, then $N \xrightarrow{s@h?v} N[s@h \mapsto v]$, with $M[s@h \mapsto v] \approx N[s@h \mapsto v]$, and there is nothing else to prove. Otherwise, we have $\mathrm{redi}(N') < \mathrm{redi}(N)$. By Lemma 1 it follows that $\mathrm{redi}(M) = \mathrm{redi}(M[s@h \mapsto v])$. Thus, $\mathrm{redi}(M[s@h \mapsto v]) + \mathrm{redi}(N') < \mathrm{redi}(M) + \mathrm{redi}(N)$. Hence $(M[s@h \mapsto v], N') \prec (M, N)$. By inductive hypothesis we know that $M[s@h \mapsto v][r@k \mapsto w] \approx N'[r@k \mapsto w]$ for any sensor r, location k and value w in the domain of r. Thus, if we choose $r = s$, $k = h$ and w the value such that $M[s@h \mapsto v][s@h \mapsto w] = M[s@h \mapsto w] = M$, then we get $M \approx N'[s@h \mapsto w]$.[3]

Finally, we need two small sub-results to conclude the proof.

- By Lemma 1 we have $\mathrm{redi}(N'[s@h \mapsto w]) = \mathrm{redi}(N')$. Since $\mathrm{redi}(N') < \mathrm{redi}(N)$ it follows that $(M, N'[s@h \mapsto w]) \prec (M, N)$. By inductive hypothesis we can close under the operator $[s@h \mapsto v]$, getting $M[s@h \mapsto v] \approx N'[s@h \mapsto w][s@h \mapsto v]$.
- Since $\approx$ is a transitive relation, $M \approx N'[s@h \mapsto w]$ and $M \approx N$, we derive that $N \approx N'[s@h \mapsto w]$. Since, $\mathrm{redi}(N) \leq \mathrm{redi}(M)$ (this was an initial assumption) and $\mathrm{redi}(N'[s@h \mapsto w]) = \mathrm{redi}(N') < \mathrm{redi}(N)$ it follows that $(N, N'[s@h \mapsto w]) \prec (M, N)$. By inductive hypothesis we can derive $N[s@h \mapsto v] \approx N'[s@h \mapsto w][s@h \mapsto v]$.

From this two facts, and by transitivity of $\approx$ we finally get $M[s@h \mapsto v] \approx N[s@h \mapsto v]$.

The proof that $\approx$ is preserved by parallel composition and channel restriction can be found in the Appendix. □

In order to prove that our labelled bisimilarity is sound with respect to reduction barbed congruence, we need the following technical result relating barbs and extensional actions.

Proposition 9. *$M \downarrow_{a@h!v}$ if and only if $M \xrightarrow{a@h!v} M$.*

Proof. It follows from the definition of rule (ActEnv). □

Theorem 3 (Soundness)**.** *Let M and N be two networks such that $M \approx N$, then $M \cong N$.*

Proof. We recall that $\cong$ is defined as the largest symmetric reduction which is reduction closed, barb preserving and contextual.

Let us prove that the labelled bisimilarity is reduction closed. Suppose that $M \rightarrowtriangle M'$. Then we have two cases: either $M \rightarrowtriangle_{\tau} M'$ or $M \rightarrowtriangle_{\sigma} M'$. In the first case Theorem 1 implies $M \xrightarrow{\tau} \equiv M'$. As $M \approx N$ there exists N' such that $N \Rightarrow N'$ and $M' \approx N'$. Now, by Theorem 1 we have that each of the τ-actions in the sequence $N \Rightarrow N'$ can be rewritten in terms of $\rightarrowtriangle_{\tau}$. Thus the entire sequence $N \Rightarrow N'$ ca be rewritten as a

[3] By Definition 5 w must be the value associated to the sensor s located at h in M, if defined. Otherwise it can be any admissible value for s.

sequence of instantaneous reductions $N \rightarrowtriangle_{\tau}^{*} N'$, which is a particular case of $N \rightarrowtriangle^{*} N'$, with $N' \approx M'$. Let us conder now the second case: $M \rightarrowtriangle_{\sigma} M'$. By Theorem 1 it follows that $M \xrightarrow{\sigma}\equiv M'$. As $M \approx N$ there exists N' such that $N \stackrel{\sigma}{\Longrightarrow} N'$ and $N' \approx M'$. By several applications of Theorem 1 we get $N \rightarrowtriangle_{\tau}^{*}\rightarrowtriangle_{\sigma}\rightarrowtriangle_{\tau}^{*} N'$. Thus, $N \rightarrowtriangle^{*} N'$, with $M' \approx N'$.

The proof that $\approx$ is closed with respect to $M \rightarrowtriangle_{a} N$ is similar.

From reduction closure and Proposition 9 it follows immediately that $\approx$ is barb preserving.

Theorem 2 says that our labelled bisimilarity is contextual.

As $\cong$ is defined as the largest relation which is reduction closed, barb-preserving and contextual, it follows that $\approx \subseteq \cong$. □

Next, we prove now that our bisimilarity is also complete. The proof relies on showing that for each extensional action α it is possible to exhibit a test T_{α} which determines whether or not a system M can perform the action α. We need a technical lemma to cut down observing contexts.

Lemma 2. *Let M and N be two networks. Let $O = n[\mathscr{I} \bowtie a!v.\mathsf{nil}]^{\mathsf{s}}_{k}$, for an arbitrary node name n, an arbitrary actuator a, and arbitrary values v and w, in the domain of a, such that $\mathscr{I}$ is only defined for a and $\mathscr{I}(a) = w \neq v$. If both $M \mid O$ and $N \mid O$ are well-formed and $M \mid O \cong N \mid O$ then $M \cong N$.*

Theorem 4 (Completeness)**.** *Let M and N such that $M \cong N$, then $M \approx N$.*

Proof. We show that relation $\mathscr{R} = \{(M,N) \mid M \cong N\}$ is a bisimulation up to $\equiv$. Let us consider two networks M and N such that $(M,N) \in \mathscr{R}$. We proceed by case analysis on the possible extensional actions of M (the case when N moves first is similar).

First, we consider *logical transitions*.

- Let us suppose that $M \xrightarrow{a} M'$. By Theorem 1 we derive $M \rightarrowtriangle_{a} M'$. Let us define the test T_a:

$$T_a \stackrel{\text{def}}{=} n[\mathscr{J} \bowtie b!1]^{\mathsf{s}}_{k}$$

  where n is a fresh node name and b is a fresh actuator such that $\mathscr{J}(b) = 0$. By Proposition 2, no σ-move can fire if a reduction $\rightarrowtriangle_{b}$ is possible. Thus, the presence of a barb $\Downarrow_{b@k!0}$ means that no σ-actions have occurred yet. Since $M \rightarrowtriangle_{a} M'$, we can apply rule (parn) to infer $M \mid T_a \rightarrowtriangle_{a} M' \mid T_a$, with $M' \mid T_a \downarrow_{b@k!0}$. As $M \cong N$ and the relation $\cong$ is both contextual and reduction closed, it follows that $N \mid T_a \rightarrowtriangle^{*}\rightarrowtriangle_{a}\rightarrowtriangle^{*} \hat{N}$, for some $\hat{N}$, with $M' \mid T_a \cong \hat{N}$. As a consequence, $\hat{N} \Downarrow_{b@k!0}$. This implies that $\hat{N} \equiv N' \mid T_a$ for some N', such that $N \mid T_a \rightarrowtriangle^{*}\rightarrowtriangle_{a}\rightarrowtriangle^{*} N' \mid T_a$, with $N \rightarrowtriangle^{*}\rightarrowtriangle_{a}\rightarrowtriangle^{*} N'$, and $M' \mid T_a \cong N' \mid T_a$. As the presence of a barb $\Downarrow_{b@k!0}$ ensures that no σ-actions have occurred, it follows that $N \rightarrowtriangle_{\tau}^{*}\rightarrowtriangle_{a}\rightarrowtriangle_{\tau}^{*} N'$. By several applications of Theorem 1 it follows that $N \stackrel{a}{\Longrightarrow}\equiv N'$ (this relies on the straightforward result that $\equiv$ is a strong bisimulation). By $M' \mid T_a \cong N' \mid T_a$ and Lemma 2 we derive $M' \cong N'$. This implies that $M' \equiv \mathscr{R} \equiv N'$.

- Let us suppose that $M \xrightarrow{\tau} M'$. This case is similar to the previous one with $T_{\tau} = T_a$.

- Let us suppose that $M \xrightarrow{\sigma} M'$. By Theorem 1 we derive $M \rightarrowtriangle_{\sigma} M'$. As $M \cong N$, by Proposition 5 there exists N' such that $N \rightarrowtriangle_{\tau}^{*}\rightarrowtriangle_{\sigma}\rightarrowtriangle_{\tau}^{*} N'$ and $M' \cong N'$. By several applications of Theorem 1 we obtain $N \stackrel{\sigma}{\Longrightarrow}\equiv N'$. As $M' \cong N'$, it follows that $M' \equiv \mathscr{R} \equiv N'$.

- Let us suppose that $M \xrightarrow{\bar{c}v\triangleright k} M'$. This transition can only be derived by an application of rule (SndObs) if $M \xrightarrow{\bar{c}v@h} M'$, for some h, such that $\mathsf{d}(h,k) \leq \mathrm{rng}(c)$. Let us build up a context that is capable to observe the action $\bar{c}v \triangleright k$. We define testing term $T_{\bar{c}v\triangleright k}$. For simplicity, in the following we abbreviate it with T:

$$T \stackrel{\text{def}}{=} m[\mathscr{J} \bowtie \lfloor c(x).[x = v]b!1.b!0;\mathsf{nil}\rfloor \mathsf{nil}]^{\mathsf{s}}_{k}$$

where m is a fresh node name and b is a fresh actuator name such that $\mathscr{J}(b) = 0$. The intuition behind this testing process is the following: T has barb $\Downarrow_{b@k!1}$ only if the communication along c has already occurred and no time actions have been fired (Proposition 2).

Since $\cong$ is contextual, $M \cong N$ implies $M \mid T \cong N \mid T$. From $M \xrightarrow{\bar{c}v@h} M'$ we can easily infer $M \mid T \xrightarrow{\tau}\xrightarrow{b} M' \mid T'$, with $T' = m[\mathscr{J}[b \mapsto 1] \bowtie b!0.\mathsf{nil}]^{\mathsf{s}}_{k}$. Notice that $M' \mid T' \downarrow_{b@k!1}$. By Theorem 1, we derive $M \mid T \mathrel{-\!\!\triangleright}_{\tau}\mathrel{-\!\!\triangleright}_{b} M' \mid T'$. As $M \mid T \cong N \mid T$ it follows that $N \mid T \mathrel{-\!\!\triangleright}^{*}\mathrel{-\!\!\triangleright}_{b}\mathrel{-\!\!\triangleright}^{*} \hat{N}$, with $\hat{N} \Downarrow_{b@k!1}$. This implies that $\hat{N} \equiv N' \mid T'$, for some N'. Furthermore, no timed actions have occurred in the reduction sequence, and hence: $N \mid T \mathrel{-\!\!\triangleright}^{*}_{\tau}\mathrel{-\!\!\triangleright}_{b}\mathrel{-\!\!\triangleright}^{*}_{\tau} N' \mid T'$. By several applications of Theorem 1 we obtain $N \mid T \Rightarrow\xrightarrow{b}\Rightarrow\equiv N' \mid T'$. This implies that $N \xRightarrow{\bar{c}v@h'}\equiv N'$, for some h' such that $\mathsf{d}(h',k) \leq \mathrm{rng}(c)$. By an application of rule (SndObs) we get $N \xRightarrow{\bar{c}v\triangleright k}\equiv N'$. From $M' \mid T \cong N' \mid T$ and Lemma 2 we derive $M' \cong N'$. This allows us to derive that $M' \equiv \mathscr{R} \equiv N'$.

- The case of $M \xrightarrow{cv\triangleright k} M'$, is similar to the previous one. The observing term is

$$T_{cv\triangleright k} \stackrel{\text{def}}{=} m[\mathscr{J} \bowtie \lfloor \bar{c}\langle v\rangle.b!1.b!0.\mathsf{nil}\rfloor \mathsf{nil}]^{\mathsf{s}}_{k}$$

where m is a fresh node name and b is a fresh actuator name such that $\mathscr{J}(b) = 0$.

Let us now consider *physical transitions*. Here, as already explained in Section 2.3, we will not provide an observing context as our language for IoT systems does not allow us to write physical observers.

- Let $M \xrightarrow{a@h!v} M'$. Since this transition can be only derived by an application of rule (ActEnv), it follows that $M' = M$ and $M \downarrow_{a@h!v}$. By Proposition 6 we obtain $N \downarrow_{a@h!v}$. By applying again rule (ActRead) to N, we obtain $N \xrightarrow{a@h!v} N' = N$ with $(M',N') \in \mathscr{R}$.
- Let $M \xrightarrow{s@h?v} M'$. Since this transition can be only derived by an application of rule (SenEnv), it follows that $M' = M[s@h \mapsto v]$. By an application of the same rule (SensEnv) we obtain $N \xrightarrow{s@h?v} N' = N[s@h \mapsto v]$. As $\cong$ is contextual we have $M[s@h \mapsto v] \cong N[s@h \mapsto v]$. This implies that $(M',N') \in \mathscr{R}$.

□

By Theorem 3 and Theorem 4 we derive the full abstraction result: reduction barbed congruence coincides with our labelled bisimilarity.

Theorem 5 (Full abstraction)**.** *$M \approx N$ if and only if $M \cong N$.*

Remark 2. *A consequence of Theorem 5 and Remark 1 is that our bisimulation proof-technique remains sound in a setting where nondeterministic sensor updates are replaced by some specific model for sensors.*

5.1 Algebraic laws and examples

As testbed for our bisimulation proof-technique we prove a number of algebraic laws on well-formed networks. Some of these laws are valid with respect to a stronger form of bisimilarity which takes into account the number of τ-actions performed by a process. The *expansion* relation [2], written $\lesssim$, is an asymmetric variant of $\approx$ such that $P \lesssim Q$ holds if $P \approx Q$ and Q has at least as many τ-moves as P.

Theorem 6 (Some algebraic laws)**.**

1. *$n[\mathscr{I} \bowtie a!v.P \mid R]^{\mu}_{h} \gtrsim n[\mathscr{I} \bowtie P \mid R]^{\mu}_{h}$, if $\mathscr{I}(a) = v$ and a does not occur in R*

2. $n[\mathscr{I} \bowtie @(x).P \mid R]_h^{\mu} \gtrsim n[\mathscr{I} \bowtie \{^h/_x\}P \mid R]_h^{\mu}$
3. $n[\mathscr{I} \bowtie \lfloor \overline{c}\langle v \rangle.P \rfloor S \mid \lfloor c(x).Q \rfloor T \mid R]_h^{\mu} \gtrsim n[\mathscr{I} \bowtie P \mid Q\{^v/_x\} \mid R]_h^{\mu}$, *if* c *is not in* R *and* $\mathrm{rng}(c) = -1$
4. $(\nu c)(n[\mathscr{I} \bowtie \lfloor \overline{c}\langle v \rangle.P \rfloor S \mid R]_h^{\mu} \mid m[\mathscr{J} \bowtie \lfloor c(x).Q \rfloor T \mid U]_k^{\mu'})$
   $\gtrsim (\nu c)(n[\mathscr{I} \bowtie P \mid R]_h^{\mu} \mid m[\mathscr{J} \bowtie Q\{^v/_x\} \mid U]_k^{\mu'})$ *if* $\mathrm{rng}(c){=}\infty$ *and* c *does not occur in* R *and* U
5. $n[\mathscr{I} \bowtie P]_h^{\mu} \approx n[\mathscr{I} \bowtie \mathsf{nil}]_h^{\mu}$ *if subterms* $\lfloor \pi.P_1 \rfloor P_2$ *or* $a!v.P_1$ *do not occur in* P
6. $n[\mathscr{I} \bowtie \mathsf{nil}]_h^{\mu} \approx \mathbf{0}$ *if* $\mathscr{I}(a)$ *is undefined for any actuator* a
7. $n[\emptyset \bowtie P]_h^{\mathtt{m}} \approx m[\emptyset \bowtie P]_k^{\mathtt{s}}$ *if* P *does not contain terms of the form* $@(x).Q$, *and for any channel* c *in* P *either* $\mathrm{rng}(c){=}\infty$ *or* $\mathrm{rng}(c) = -1$.

Laws 1-4 are a sort of tau-laws. Laws 5 and 6 models garbage collection of processes and nodes, respectively. Law 7 gives a sufficient condition for node anonymity as well as for non-observable node mobility.

Next, we show that our labelled bisimilarity can be used to deal with more complicated systems. In the following, we apply non-trivial up to expansion proof-techniques [37] to formally prove that the two systems Sys and $\overline{Sys}$ mentioned in Proposition 8 are bisimilar (up to an obvious channel restriction). In this respect, the first four laws of Theorem 6 are fundamentals.

The following lemma basically says that, under specific conditions, our bisimilarity is preserved by parallel composition on processes within nodes.

Lemma 3. *If* $(\nu \tilde{c})\big(n[\mathscr{I} \bowtie P_1]_h^{\mu} \mid O_1\big) \approx (\nu \tilde{d})\big(n[\mathscr{I} \bowtie P_2]_k^{\mu} \mid O_2\big)$ *then* $(\nu \tilde{c})\big(n[\mathscr{I} \bowtie P_1 \mid R]_h^{\mu} \mid O_1\big) \approx (\nu \tilde{d})\big(n[\mathscr{I} \bowtie P_2 \mid R]_k^{\mu} \mid O_2\big)$, *for any process* R *which can only read sensors, transmit along some fresh Internet channel, and let time pass.*

We can now rely on Theorem 5 to rephrase Proposition 8 by replacing reduction barbed congruence with our labelled bisimilarity.

Proposition 10. *If* $\delta = 1$ *then* $(\nu \tilde{c})Sys \ \approx \ (\nu \tilde{c})(\nu g)\overline{Sys}$.

Proof. First of all, notice that we can focus on smaller systems. This is because:

- $(\nu \tilde{c})Sys \ = \ (\nu \tilde{c})\big(Phone \mid LM_1 \mid BM \mid LM_2\big) \ \equiv \ (\nu \tilde{c})\big(Phone \mid LM_1 \mid LM_2\big) \mid BM$
- $(\nu \tilde{c}, g)\overline{Sys} \ = \ (\nu \tilde{c}, g)\big(\overline{Phone} \mid LM_1 \mid BM \mid LM_2 \mid \overline{CLM}\big) \ \equiv \ (\nu \tilde{c}, g)\big(\overline{Phone} \mid LM_1 \mid LM_2 \mid \overline{CLM}\big) \mid BM$.

By Theorem 2 the relation $\approx$ is preserved by parallel composition. Thus, in order to prove our result it is enough to show that:

$$(\nu \tilde{c})\big(Phone \mid LM_1 \mid LM_2\big) \ \approx \ (\nu \tilde{c})(\nu g)\big(\overline{Phone} \mid LM_1 \mid LM_2 \mid \overline{CLM}\big) \ .$$

Actually, we can consider even smaller systems. As $Phone = n_P[\mathscr{I}_P \bowtie BoilerCtrl \mid LightCtrl]_{out}^{\mathtt{m}}$, $\overline{Phone} = n_P[\mathscr{I}_P \bowtie BoilerCtrl \mid \overline{LightCtrl}]_{out}^{\mathtt{m}}$, and channels c_1, c_2 and g do not occur in $BoilerCtrl$, by Lemma 3 it is enough to show that:

$$(\nu \tilde{c})\big(n_P[\mathscr{I}_P \bowtie LightCtrl]_{out}^{\mathtt{m}} \mid LM_1 \mid LM_2\big) \ \approx \ (\nu \tilde{c})(\nu g)\big(n_P[\mathscr{I}_P \bowtie \overline{LightCtrl}]_{out}^{\mathtt{m}} \mid LM_1 \mid LM_2 \mid \overline{CLM}\big) \ .$$

Let us call S_{L} the system on the left side, and S_{R} the system on the right side. Let us define the relation

$$\mathscr{R} \stackrel{\text{def}}{=} \bigcup_{i=1}^{17} \Big((\nu \tilde{c})M_i \, , \, (\nu \tilde{c})(\nu g)N_i\Big)$$

where the pairs (M_i, N_i) are given in the Appendix. We will prove that the symmetric closure of $\mathscr{R}$ is a bisimulation up to expansion [37]. The we will show that $S_{\mathrm{L}} = (\nu \tilde{c})M_1 \ \mathscr{R} \ (\nu \tilde{c})(\nu g)N_1 \lesssim S_{\mathrm{R}}$. As the up to expansion technique is sound, and the expansion relation $\lesssim$ is a transitive relation, it follows that $S_{\mathrm{L}} \approx S_{\mathrm{R}}$. The details of the proof can be found in the Appendix. □

6 Conclusions and related work

We have proposed a process calculus, called CaIT, to investigate the semantic theory of systems in the Internet of Things paradigm. The dynamics of CaIT is formalised by means of an intuitive reduction semantics and a more operational intensional semantics, which model the evolution of systems in isolation. An Harmony theorem show that these two different operational semantics coincide. An extensional semantics has then been defined to emphasize the interaction of IoT systems with the environment. The extensional semantics has been used to define a labelled bisimilarity which has been proved to be a coinductive characterisation of a natural notion of contextual equivalence. Our bisimilarity has been used to prove non-trivial system equalities.

To our knowledge, the IoT-calculus [22] is the first process calculus for IoT systems which captures the interaction between sensors, actuators and computing processes. Smart objects are represented as point-to-point communicating nodes of heterogeneous networks. The network topology is represented as a graph whose links can be nondeterministically established or destroyed. The paper contains a labelled transition system with two different kinds of transitions. The first one takes into account interactions with the physical environment, similarly to our physical transitions, but includes also topology changes. The second kind of transition models nodes activities, mainly communications, similarly to our logical transitions. The paper proposes two notions of bisimilarity: one using only the first kind of transitions and equating systems from the point of view of the end user, and a second one using all transitions and equating systems from the point of view of the other devices.

We report here the main differences between CaIT and the IoT-calculus. In CaIT, we support timed behaviours, with desirable time, consistency and fairness properties (see, for instance, Proposition 7). Both sensors and actuators in CaIT are under the control of a single entity, i.e. the controller process of the node where they are deployed. This was a security issue. The nondeterministic link entailment of the IoT-calculus makes the semantics of communication simpler than ours as it does not rely on the distance between nodes; on the other hand it does not allow to enforce that a smart device should be either in a place or in another, but never in both. This can be easily represented in CaIT (again, see Proposition 7). CaIT has a finer control of inter-node communications as they depend on nodes' distance and transmission range of channels. Node mobility in CaIT is timed constrained: in one time unit at most a fixed distance δ may be covered. Finally, Lanese et al.'s *end-user bisimilarity* shares most of the motivations of our bisimilarity. In the IoT-calculus, end users provide values to sensors and check actuators. They can also move nodes thus creating or removing connections, but they cannot observe channel communication. Thus, two systems with different connections between nodes are not end-user bisimilar. Unlike end-user bisimilarity, our notion of bisimilarity observes node mobility in a milder manner: the movements of a mobile node can be observed if the node either uses an actuator or transmits along a short-range channel or communicates its physical position. Finally, end-user bisimilarity is not preserved by parallel composition. Compositionality is recovered by observing also channel communication. The resulting bisimilarity models observation from the point of view of the other devices. Its distinguishing power is definitely stronger than that of our bisimilarity.

More recently, Bodei et al. [6] have proposed a new untimed process calculus, IOT-LYSA, supporting a control flow analysis that safely approximates the abstract behaviour of IoT systems. Essentially, they track how data spread from sensors to the logics of the network, and how physical data are manipulated. Intra-node generative communications in IoT-LYSA are implemented through a shared store à la Linda [14]. In this manner physical data are made available to software entities that analyse them and trigger the relevant actuators to perform the desired behaviour. The calculus adopt asynchronous multi-party communication among nodes taking care of node proximity (the topology is static). The dynamics of the calculus is given in terms of a reduction relation. No behavioural equivalences are defined.

Our calculus takes inspiration from algebraic models for wireless systems [23, 33, 26, 16, 15, 27, 28, 21, 24, 39, 13, 10, 7]. All these models adopt broadcast communication on partial topologies, while we consider point-to-point communication, as in [22]. Our way of modelling network topology is taken from [23, 26]. Paper [17] provides formal models for node mobility depending on the passage of time. Proposition 5 was inspired by [10]. A fully abstract observational theory for untimed ad hoc networks with broadcast communication can be found in [26, 16]. Paper [39] provides a symbolic semantics for ad hoc networks.

Vigo et al. [41] proposed a calculus for wireless-based cyber-physical (CPS) systems endowed with a theory that allows modelling and reasoning about cryptographic primitives, together with explicit notions of communication failure and unwanted communication. One of the main goal of the paper is a faithful representation denial-of-service. However, as pointed out in [43], the calculus does not provide a notion of network topology, local broadcast and behavioural equivalence. It also lacks a clear distinction between physical components (sensor and actuators) and logical ones (processes). Compared to [41], paper [43] introduces a static network topology and enrich the theory with an harmony theorem.

As already said, CaIT has some similarities with the *synchronous languages* of the Esterel family [5, 8, 3]. In this setting, computations proceed in phases called instants, which are quite similar to our time intervals. For instance, our timed reduction semantics has many points in common with that of a recent synchronous reactive language, *CRL* [3][4]. The authors define two bisimulation equivalences. The first bisimulation formalises a *fine-grained* observation of programs: the observer is viewed as a program, which is able to interact with the observed program at any point of its execution. The second reflects a *coarse-grained* observation of programs: here the observer is viewed as part of the environment, which interacts with the observed program only at the start and the end of instants. The fine-grained bisimilarity is more in the style of a bisimulation for a process calculus.

Finally, CaIT is somehow reminiscent of the SCEL language [12]. A framework to model behaviour, knowledge, and data aggregation of Autonomic Systems.

Acknowledgements We thank Ilaria Castellani and Matthew Hennessy for their precious comments on an early draft. We thank Valentina Castiglioni for an early writing of the proof of the Harmony theorem.

References

[1] R.M. Amadio. A synchronous pi-calculus. *Information and Computation*, 205(9):1470–1490, 2007.

[2] S. Arun-Kumar and M. Hennessy. An efficiency preorder for processes. *Acta Informatica*, 29:737–760, 1992.

[3] P. Attar and I. Castellani. Fine-Grained and Coarse-Grained Reactive Noninterference. In *8th TGC*, volume 8358 of *LNCS*, pages 159–179. Springer, 2013.

[4] L. Atzori, A Iera, and G Morabito. The Internet of Things: A survey. *Computer Networks*, 54(15):2787–2805, 2010.

[5] G. Berry and G. Gonthier. The Esterel Synchronous Programming Language: Design, Semantics, Implementation. *Science of Computer Programming*, 19(2):87–152, 1992.

[6] C. Bodei, P. Degano, G.L. Ferrari, and L. Galletta. Where Do Your IoT Ingredients Come From? In *COORDINATION 2016*, volume 9686 of *Lecture Notes in Computer Science*, pages 35–50. Springer, 2016.

[7] J. Borgström, S. Huang, M. Johansson, P. Raabjerg, B. Victor, J.A. Pohjola, and J. Parrow. Broadcast psi-calculi with an application to wireless protocols. *Software and System Modeling*, 14(1):201–216, 2015.

[4] The *CRL* language does not support mobility.

[8] F. Boussinot and R. de Simone. The SL Synchronous Language. *IEEE Transactions on Software Engineering*, 22(4):256–266, 1996.

[9] L. Cardelli and A. Gordon. Mobile Ambients. *Theoretical Computer Science*, 240(1):177–213, 2000.

[10] A. Cerone, M. Hennessy, and M. Merro. Modelling MAC-Layer Communications in Wireless Systems. *Logical Methods in Computer Science*, 11(1:18), 2015.

[11] S. De, T. Elsaleh, P. M. Barnaghi, and S. Meissner. An Internet of Things Platform for Real-World and Digital Objects. *Scalable Computing: Practice and Experience*, 13(1), 2012.

[12] R. De Nicola, M. Loreti, R. Pugliese, and F. Tiezzi. A Formal Approach to Autonomic Systems Programming: The SCEL language. *ACM Trans. Auton. Adapt. Syst.*, 9:7:1–7:29, 2014.

[13] A. Fehnker, R.J. van Glabbeek, P. Höfner, A. McIver, M Portmann, and W.L. Tan. A Process Algebra for Wireless Mesh Networks. In *ESOP*, volume 7211 of *LNCS*, pages 295–315. Springer, 2012.

[14] D. Gelernter. Generative communication in linda. *ACM Trans. Program. Lang. Syst.*, 7(1):80–112, 1985.

[15] F. Ghassemi, W. Fokkink, and A. Movaghar. Verification of Mobile Ad Hoc Networks: an Algebraic Approach. *Theor. Comp. Science*, 412(28):3262–3282, 2011.

[16] J.C. Godskesen. A Calculus for Mobile Ad Hoc Networks. In *COORDINATION*, volume 4467 of *LNCS*, pages 132–150. Springer, 2007.

[17] J.C. Godskesen and S. Nanz. Mobility Models and Behavioural Equivalence for Wireless Networks. In *COORDINATION*, volume 5521 of *LNCS*, pages 106–122. Springer, 2009.

[18] J. Gubbi and M. Palaniswami. Internet of Things (IoT): A vision, architectural elements, and future directions. *Fut. Gen. Comput. Syst.*, 29(7):1645–1660, 2013.

[19] M. Hennessy and T. Regan. A Process Algebra for Timed Systems. *Information and Computation*, 117(2):221–239, 1995.

[20] K. Honda and N. Yoshida. On Reduction-Based Process Semantics. *Theoretical Computer Science*, 151(2):437–486, 1995.

[21] D. Kouzapas and A. Philippou. A Process Calculus for Dynamic Networks. In *FMOODS/FORTE*, volume 6722 of *LNCS*, pages 213–227. Springer, 2011.

[22] I. Lanese, L. Bedogni, and M. Di Felice. Internet of Things: a process calculus approach. In *28th ACM SAC*, pages 1339–1346. ACM, 2013.

[23] I. Lanese and D. Sangiorgi. An Operational Semantics for a Calculus for Wireless Systems. *Theoretical Computer Science*, 411:1928–1948, 2010.

[24] R. Lanotte and M. Merro. Semantic analysis of gossip protocols for wireless sensor networks. In *22nd International Conference on Concurrency Theory (CONCUR 2011)*, volume 6901 of *Lecture Notes in Computer Science*, pages 156–170. Springer, 2011.

[25] R. Lanotte and M. Merro. A Semantic Theory of the Internet of Things (Extended Abstract). In *COORDINATION 2016*, volume 9686 of *Lecture Notes in Computer Science*, pages 157–174. Springer, 2016.

[26] M. Merro. An Observational Theory for Mobile Ad Hoc Networks (full paper). *Information and Computation*, 207(2):194–208, 2009.

[27] M. Merro, F. Ballardin, and E. Sibilio. A timed calculus for wireless systems. *Theoretical Computer Science*, 412(47):6585–6611, 2011.

[28] M. Merro and E. Sibilio. A calculus of trustworthy ad hoc networks. *Formal Aspects of Computing*, 25(5):801–832, 2013.

[29] M. Merro and F. Zappa Nardelli. Behavioral theory for mobile ambients. *Journal of the ACM*, 52(6):961–1023, 2005.

[30] R. Milner. The polyadic π-calculus: a tutorial. Technical report, LFCS, 1991.

[31] R. Milner and D. Sangiorgi. Barbed Bisimulation. In *19th ICALP*, volume 623 of *LNCS*, pages 685–695. Springer, 1992.

[32] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7):1497–1516, 2012.

[33] S. Nanz and C. Hankin. A Framework for Security Analysis of Mobile Wireless Networks. *Theoretical Computer Science*, 367(1-2):203–227, 2006.

[34] M. P. Papazoglou and W. van den Heuvel. Service oriented architectures: approaches, technologies and research issues. *The VLDB Journal*, 16(3):389–415, 2007.

[35] G. Plotkin. A structural approach to operational semantics. Report DAIMI FN-19, Aarhus University, 1981.

[36] G Roussos and V. Kostakos. RFID in pervasive computing: State-of-the-art and outlook. *Pervasive and Mobile Computing*, 5(1):110–131, 2009.

[37] D. Sangiorgi and D. Walker. *The Pi-Calculus-a theory of mobile processes*. Cambridge University Press, 2001.

[38] A.V.D. Schaft and H. Schumacher. *An introduction to hybrid dynamical systems*, volume 251 of *Lecture Notes in Control and Information Science*. Springer, 2000.

[39] A. Singh, C.R. Ramakrishnan, and S.A. Smolka. A process calculus for Mobile Ad Hoc Networks. *Science of Computer Programming*, 75(6):440–469, 2010.

[40] B. Sundararaman, U. Buy, and A. D. Kshemkalyani. Clock Synchronization for Wireless Sensor Networks: a Survey. *Ad Hoc Networks*, 3(3):281–323, 2005.

[41] R. Vigo, F. Nielson, and H.R. Nielson. Broadcast, Denial-of-Service, and Secure Communication. In *IFM*, volume 7940 of *LNCS*, pages 412–427. Springer, 2013.

[42] G. Wang, G. Cao, and T.F. La Porta. Movement-Assisted Sensor Deployment. *IEEE Transactions on Mobile Computing*, 5(6):640–652, 2006.

[43] X. Wu and H. Zhu. A Calculus for Wireless Sensor Networks from Quality Perspective. In *IEE HASE*, pages 223–231, 2015.

A Proofs

A.1 Proofs of Section 2

In order to prove Proposition 1 we need a technical lemma on time determinism of nodes.

Lemma 4. *If* $n[P]^{\mu}_{h} \rightarrowtriangle_{\sigma} n'[P']^{\mu'}_{h'}$ *and* $n[P]^{\mu}_{h} \rightarrowtriangle_{\sigma} n''[P'']^{\mu''}_{h''}$ *then* $n = n' = n''$*,* $P' \equiv P''$*,* $\mu = \mu' = \mu''$ *and* $\mathrm{d}(h', h'') \leq 2\delta$*.*

Proof. By structural induction on P. □

Proof of Proposition 1

Proof. The proof is by rule induction on why $M \rightarrowtriangle_{\sigma} M'$. The most significant case is when $M \rightarrowtriangle_{\sigma} M'$ is derived by an application of rule (timemob):

$$\frac{n[\mathscr{I} \bowtie \prod_{i\in I} \lfloor \pi_i.P_i \rfloor Q_i \mid \prod_{j\in J} \sigma.P_j]^{\mathtt{m}}_{k} \not\rightarrowtriangle_{\tau} \qquad \mathrm{d}(k,k') \leq \delta}{n[\mathscr{I} \bowtie \prod_{i\in I} \lfloor \pi_i.P_i \rfloor Q_i \mid \prod_{j\in J} \sigma.P_j]^{\mathtt{m}}_{k} \rightarrowtriangle_{\sigma} n[\mathscr{I} \bowtie \prod_{i\in I} Q_i \mid \prod_{j\in J} P_j]^{\mathtt{m}}_{k'}}$$

with $M = n[\mathscr{I} \bowtie \prod_{i\in I} \lfloor \pi_i.P_i \rfloor Q_i \mid \prod_{j\in J} \sigma.P_j]^{\mathtt{m}}_{k}$ and $M' = n[\mathscr{I} \bowtie \prod_{i\in I} Q_i \mid \prod_{j\in J} P_j]^{\mathtt{m}}_{k'}$. Suppose there exists M'' such that $M \rightarrowtriangle_{\sigma} M''$. Notice that, due to its structure, network M may perform a timed reduction only by an application of rule (timemob). Thus, by rule (timemob) we would have:

$$\frac{n[\mathscr{I} \bowtie \prod_{i\in I} \lfloor \pi_i.P_i \rfloor Q_i \mid \prod_{j\in J} \sigma.P_j]^{\mathtt{m}}_{k} \not\rightarrowtriangle_{\tau} \qquad \mathrm{d}(k,k'') \leq \delta}{n[\mathscr{I} \bowtie \prod_{i\in I} \lfloor \pi_i.P_i \rfloor Q_i \mid \prod_{j\in J} \sigma.P_j]^{\mathtt{m}}_{k} \rightarrowtriangle_{\sigma} n[\mathscr{I} \bowtie \prod_{i\in I} Q''_i \mid \prod_{j\in J} P''_j]^{\mathtt{m}}_{k''}}$$

with $M'' = n[\mathscr{I} \bowtie \prod_{i \in I} Q''_i \mid \prod_{j \in J} P''_j]^{\mathfrak{m}}_{k''}$. By Lemma 4 it follows that $\prod_{i \in I} Q_i \mid \prod_{j \in J} P_j \equiv \prod_{i \in I} Q''_i \mid \prod_{j \in J} P''_j$. Moreover, by triangular inequality it holds that $\mathrm{d}(k', k'') \leq \mathrm{d}(k, k') + \mathrm{d}(k, k'') \leq 2\delta$.

The other cases are similar. □

In order to prove maximal progress we need two simple lemmas.

Lemma 5. *If* $\prod_{i \in I} n_i[\mathscr{I}_i \bowtie P_i]^{\mu_i}_{h_i} \rightarrowtriangle_{\tau} M$ *then* $\prod_{i \in I} n_i[\mathscr{I}_i \bowtie P_i \mid Q_i]^{\mu_i}_{h_i} \rightarrowtriangle_{\tau} N$*, for some* N.

Lemma 6. *If* $n[P]^{\mu}_{h} \not\rightarrowtriangle_{\sigma}$ *then for any process* Q *we have* $n[P \mid Q]^{\mu}_{h} \not\rightarrowtriangle_{\sigma}$.

Proof of Proposition 2

Proof. The proof is by rule induction on why $M \rightarrowtriangle_{\mathrm{i}} M'$. The most involved case is when $M \rightarrowtriangle_{\mathrm{i}} M'$ is derived by an application of rule (parp). This means that

$$M = \prod_{i \in I} n_i[\mathscr{I}_i \bowtie P_i \mid Q_i]^{\mu_i}_{h_i} \rightarrowtriangle_{\mathrm{i}} \prod_{i \in I} n_i[\mathscr{I}'_i \bowtie P'_i \mid Q_i]^{\mu_i}_{h'_i} = M'$$

because $\prod_{i \in I} n_i[\mathscr{I}_i \bowtie P_i]^{\mu_i}_{h_i} \rightarrowtriangle_{\mathrm{i}} \prod_{i \in I} n_i[\mathscr{I}'_i \bowtie P'_i]^{\mu_i}_{h'_i}$. By inductive hypothesis $\prod_{i \in I} n_i[\mathscr{I}_i \bowtie P_i]^{\mu_i}_{h_i} \not\rightarrowtriangle_{\sigma}$. We recall that rule (timepar) is the only one yielding timed reductions on parallel networks. Thus, if $\prod_{i \in I} n_i[\mathscr{I}_i \bowtie P_i]^{\mu_i}_{h_i} \not\rightarrowtriangle_{\sigma}$ it means that rule (timepar) could not be applied. Then, there are only two possibilities.

- Either $\prod_{i \in I} n_i[\mathscr{I}_i \bowtie P_i]^{\mu_i}_{h_i} \rightarrowtriangle_{\tau} N$, for some N. Then by Lemma 5 we obtain $M \rightarrowtriangle_{\tau} N'$, for some N'. As rule (timepar) is the only rule yielding timed reductions from parallel networks, it follows that $M \not\rightarrowtriangle_{\sigma}$.
- Or $n_j[\mathscr{I}_j \bowtie P_j]^{\mu_j}_{h_j} \not\rightarrowtriangle_{\sigma}$, for some $j \in I$. Then by Lemma 6 we have $n_j[\mathscr{I}_j \bowtie P_j \mid Q_j]^{\mu_j}_{h_j} \not\rightarrowtriangle_{\sigma}$. As rule (timepar) is the only rule yielding timed reductions from parallel networks, it follows that $M \not\rightarrowtriangle_{\sigma}$.

The remaining cases work smoothly. □

Proof of Proposition 3

Proof. The proof is by contradiction. We suppose there is no N such that $M \rightarrowtriangle_{\sigma} N$ and we prove that there is M' such that $M \rightarrowtriangle_{\mathrm{i}} M'$. We proceed by induction on the structure of M.

- Let $M = \mathbf{0}$. This case is not admissible because by an application or rule (timezero) we derive $M \rightarrowtriangle_{\sigma} M$.
- Let $M = n[P]^{\mu}_{h}$. As $M \not\rightarrowtriangle_{\sigma}$ and (timestat) and (timemob) are the the only rules that could be used to derive a timed reduction from M, it follows that there are two possibilities.
  - Either $M \rightarrowtriangle_{\tau} M'$, for some M', and we are done.
  - Or P has not the proper structure for applying rule (timestat) or rule (timemob). This means that $P \equiv P_1 \mid P_2$, with $P_1 = \rho.P'_1$ and $\rho \in \{@(x), s?(x), a!v\}$. In this case, by an application of one among the rules (pos), (sensread), (actunchg), and (actchg), followed by an application of rule (parp), we can infer $M \rightarrowtriangle_{\mathrm{i}} M'$, for some M'.
- Let $M = M_1 \mid M_2$, for some M_1 and M_2. As $M \not\rightarrowtriangle_{\sigma}$ and (timepar) is the only rule which could be used to derive a timed reduction from M, it follows that there are two possibilities.
  - Either $M \rightarrowtriangle_{\tau} M'$, for some M'; hence $M \rightarrowtriangle_{\mathrm{i}} M'$ and we are done.
  - Or at least one among M_1 and M_2 cannot perform a timed reduction. Suppose $M_1 \not\rightarrowtriangle_{\sigma}$; by inductive hypothesis there is M'_1 such that $M_1 \rightarrowtriangle_{\mathrm{i}} M'_1$. By an application of rule (parn) we derive $M \rightarrowtriangle_{\mathrm{i}} M'_1 \mid M_2$.
- Let $M = (\nu c)M_1$. This case requires an easy application of the inductive hypothesis.

□

In order to prove Proposition 4, we need a couple of technical definitions and lemmas.

Definition 9. *Let* $\mathrm{pfxi}()$ *be the function that given a process P returns an upper bound to the number of the* untimed prefixes *that can give rise to an instantaneous reduction when P is plugged in a node.*

$$\begin{array}{rclrclrcl}
\mathrm{pfxi}(\mathsf{nil}) & \stackrel{\text{def}}{=} & 0 & \mathrm{pfxi}(\sigma.P) & \stackrel{\text{def}}{=} & 0 & \mathrm{pfxi}(\rho.P) & \stackrel{\text{def}}{=} & 1+\mathrm{pfxi}(P) \ (\textit{if}\ \rho \neq \sigma) \\
\mathrm{pfxi}(X) & \stackrel{\text{def}}{=} & \infty & \mathrm{pfxi}(\mathsf{fix}X.P) & \stackrel{\text{def}}{=} & \mathrm{pfxi}(P) & \mathrm{pfxi}(\lfloor \pi.P \rfloor Q) & \stackrel{\text{def}}{=} & 1+\mathrm{pfxi}(P) \\
\end{array}$$

$$\mathrm{pfxi}([b]P;Q) \stackrel{\text{def}}{=} \max(\mathrm{pfxi}(P),\mathrm{pfxi}(Q)) \qquad \mathrm{pfxi}(P \mid Q) \stackrel{\text{def}}{=} \mathrm{pfxi}(P)+\mathrm{pfxi}(Q)$$

Lemma 7. *For any closed process P,* $\mathrm{pfxi}(P)$ *is finite.*

Proof. The proof is by structural induction on P. The only interesting case is when $P = \mathsf{fix}X.P_1$, as P_1 may contain the process variable X and $\mathrm{pfxi}(X) = \infty$. However, in our calculus we only admit time-guarded recursion. Thus, X may occur in P_1 only if guarded by at least one σ prefix, and $\mathrm{pfxi}(\sigma.Q) = 0$, for any Q. It follows that $\mathrm{pfxi}(\mathsf{fix}X.P_1) \in \mathbb{N}$, for any P_1. □

Now, we lift the previous definition to systems.

Definition 10. *Let us define a function* $\mathrm{redi}()$ *that given a network M returns an upper bound to the number of consecutive instantaneous reductions that M may perform:*

$$\begin{array}{rclrcl}
\mathrm{redi}(\mathbf{0}) & \stackrel{\text{def}}{=} & 0 & \mathrm{redi}(n[\mathscr{I} \bowtie P]^{\mu}_{h}) & \stackrel{\text{def}}{=} & \mathrm{pfxi}(P) \\
\mathrm{redi}((\nu c)M) & \stackrel{\text{def}}{=} & \mathrm{redi}(M) & \mathrm{redi}(M \mid N) & \stackrel{\text{def}}{=} & \mathrm{redi}(M)+\mathrm{redi}(N) \ .
\end{array}$$

From Lemma 7 can be easily proved that $\mathrm{redi}(M)$ is always finite.

Lemma 8. *For any network M,* $\mathrm{redi}(M)$ *is finite.*

The proof of Proposition 4 is by induction on the structure of M; it follows from Lemma 8.

A.2 Proofs of Section 3

Let us prove Proposition 7. For that we need a technical lemma.

Lemma 9. *If* $Sys\ (\rightarrowtriangle_{\mathrm{i}}^{*}\rightarrowtriangle_{\sigma})^{*}\ Sys'$ *then* $Sys' \equiv Phone' \mid Home'$ *where:*

- $Phone' = n_P[\mathscr{I}_P \bowtie BoilerCtrl \mid LightCtrl]^{\mathtt{m}}_{l'}$*, for some* l'*, with* $\mathscr{I}_P(mode) = \mathsf{auto}$
- $Home' = LR_1 \mid LR_2 \mid BoilerMng$*, for some* LR_1 *and* LR_2*,*
- $BoilerMng = n_B[\mathscr{I}_B \bowtie BoilerMng]^{\mathtt{s}}_{loc2}$*, with* $\mathscr{I}_B(temp) = \Theta$*.*

Proof. The proof is by mathematical induction on the integer j such that $Sys\ (\rightarrowtriangle_{\mathrm{i}}^{*}\rightarrowtriangle_{\sigma})^{j}\ Sys'$.

The case $j = 0$ is trivial.

Let us move on the inductive case. Let $Sys\ (\rightarrowtriangle_{\mathrm{i}}^{*}\rightarrowtriangle_{\sigma})^{j}\ Sys_1$, for $j > 0$. By inductive hypothesis we have: $Sys_1 \equiv Phone_1 \mid Home_1$ where:

- $Phone_1 = n_P[\mathscr{I}_P \bowtie BoilerCtrl \mid LightCtrl]^{\mathtt{m}}_{l_1}$, for some l_1, with $\mathscr{I}_P(mode) = \mathsf{auto}$
- $Home_1 = LR_1 \mid LR_2 \mid BoilerMng$, for some LR_1 and LR_2,
- $BoilerMng = n_B[\mathscr{I}_B \bowtie BoilerMng]^{\mathtt{s}}_{loc2}$, with $\mathscr{I}_B(temp) = \Theta$.

We recall that sensor changes are not modelled in the reduction semantics as they require the intervention of the physical environment. Thus, the value of all sensors will remain unchanged during the reduction sequence. We show that whenever $Sys_1 \rightarrowtriangle_{\mathrm{i}}^{*} \rightarrowtriangle_{\sigma} Sys'$, then Sys' has still the same structure as Sys_1. Let us consider a portion of Sys_1 composed by the phone and the boiler manager. Then, we have the following sequence of instantaneous reductions. We recall that $\mathcal{I}_P(mode) = \mathsf{auto}$ and $\mathcal{I}_B(temp) = \Theta$.

$$\begin{array}{rl}
\multicolumn{2}{l}{Phone_1 \,\big|\, BoilerMng} \\
= & n_P[\mathcal{I}_P \bowtie BoilerCtrl \mid LightCtrl]^{\mathtt{m}}_{l_1} \;\big|\; n_B[\mathcal{I}_B \bowtie BoilerMng]^{\mathtt{s}}_{loc2} \\
\rightarrowtriangle_{\mathrm{i}} & n_P[\mathcal{I}_P \bowtie \lfloor \overline{b}\langle \mathsf{auto}\rangle.\sigma.BoilerCtrl \rfloor \ldots \mid LightCtrl]^{\mathtt{m}}_{l_1} \;\big|\; n_B[\mathcal{I}_B \bowtie BoilerMng]^{\mathtt{s}}_{loc2} \\
\rightarrowtriangle_{\mathrm{i}} & n_P[\mathcal{I}_P \bowtie \sigma.BoilerCtrl \mid LightCtrl]^{\mathtt{m}}_{l_1} \;\big|\; n_B[\mathcal{I}_B \bowtie TempCtrl]^{\mathtt{s}}_{loc2} \\
\rightarrowtriangle_{\mathrm{i}} & n_P[\mathcal{I}_P \bowtie \sigma.BoilerCtrl \mid LightCtrl]^{\mathtt{m}}_{l_1} \;\big|\; n_B[\mathcal{I}_B \bowtie boiler!\mathsf{off}.\sigma.BoilerMng]^{\mathtt{s}}_{loc2} \\
\rightarrowtriangle_{\mathrm{i}} & n_P[\mathcal{I}_P \bowtie \sigma.BoilerCtrl \mid LightCtrl]^{\mathtt{m}}_{l_1} \;\big|\; n_B[\mathcal{I}_B[boiler \mapsto \mathsf{off}] \bowtie \sigma.BoilerMng]^{\mathtt{s}}_{loc2} \\
= & n_P[\mathcal{I}_P \bowtie \sigma.BoilerCtrl \mid LightCtrl]^{\mathtt{m}}_{l_1} \;\big|\; n_B[\mathcal{I}_B \bowtie \sigma.BoilerMng]^{\mathtt{s}}_{loc2} \;\; .
\end{array}$$

Now, both the phone and the boiler manager can only perform a timed reduction. However, the whole system may have further instantaneous reductions depending whether the phone is in position to interact with the light managers of the house. In any case, thanks to (i) *well-timedness* (Proposition 4), (ii) *patience* (Proposition 3), (iii) rule (parn), (iv) rule (struct) we will eventually have a reduction sequence of the form:

$$Phone_1 \,\big|\, LR_1 \,\big|\, LR_2 \,\big|\, BoilerMng \;\; \rightarrowtriangle_{\mathrm{i}}^{*} \rightarrowtriangle_{\sigma} \;\; Phone' \,\big|\, LR_1' \,\big|\, LR_2' \,\big|\, BoilerMng$$

in which $\mathcal{I}_P(mode) = \mathsf{auto}$ and $\mathcal{I}_B(temp) = \Theta$ (the reduction semantics cannot change sensor values) and $Phone'$ is exactly as $Phone_1$ except for the fact that is located at a possibly new location l', with $\mathsf{d}(l_1, l') \leq 1$. □

Proof of Proposition 7

Proof. By Lemma 9 we deduce that Sys' preserves the structure of Sys and also the value of its sensors. Let us prove the four cases of the proposition, one by one.

1. Let us consider the evolution of $Sys'[mode \mapsto \mathsf{man}]$. By inspection on the definitions in Table 4 it is easy to derive that

$$\begin{array}{rcl}
Sys'[mode \mapsto \mathsf{man}] & \equiv & Phone'[mode \mapsto \mathsf{man}] \mid LR_1 \mid LR_2 \mid n_B[\mathcal{I}_B \bowtie BoilerMng]^{\mathtt{s}}_{loc2} \\
 & \rightarrowtriangle_{\mathrm{i}}^{*} \rightarrowtriangle_{\sigma} & Phone'[mode \mapsto \mathsf{man}] \mid LR_1' \mid LR_2' \mid n_B[\mathcal{I}_B' \bowtie BoilerManual]^{\mathtt{s}}_{loc2}
\end{array}$$

with $\mathcal{I}_B'(boiler) = \mathsf{on}$.

2. Let us consider the evolution of $Sys'[temp \mapsto t]$, with $t < \Theta$. We spell out this case in more detail. We recall that the sensor *mode* of the phone is set to auto. We also recall that, by an application of rules (parn) and (struct), if a parallel component can execute an instantaneous reduction then the whole network can execute the same reduction. Thus, in following we concentrate on the reductions deriving from the phone and the boiler manager when $t < \Theta$.

$$\begin{array}{rl}
\multicolumn{2}{l}{(Phone' \;\big|\; BoilerMng)[temp \mapsto t]} \\
= & n_P[\mathcal{I}_P \bowtie BoilerCtrl \mid LightCtrl]^{\mathtt{m}}_{l'} \;\big|\; n_B[\mathcal{I}_B[temp \mapsto t] \bowtie BoilerMng]^{\mathtt{s}}_{loc2} \\
\rightarrowtriangle_{\mathrm{i}} & n_P[\mathcal{I}_P \bowtie \lfloor \overline{b}\langle \mathsf{auto}\rangle.\sigma.BoilerCtrl \rfloor \ldots \mid LightCtrl]^{\mathtt{m}}_{l'} \;\big|\; n_B[\mathcal{I}_B' \bowtie BoilerMng]^{\mathtt{s}}_{loc2} \\
\rightarrowtriangle_{\mathrm{i}} & n_P[\mathcal{I}_P \bowtie \sigma.BoilerCtrl \mid LightCtrl]^{\mathtt{m}}_{l'} \;\big|\; n_B[\mathcal{I}_B' \bowtie TempCtrl]^{\mathtt{s}}_{loc2} \\
\rightarrowtriangle_{\mathrm{i}} & n_P[\mathcal{I}_P \bowtie \sigma.BoilerCtrl \mid LightCtrl]^{\mathtt{m}}_{l'} \;\big|\; n_B[\mathcal{I}_B' \bowtie boiler!\mathsf{on}.\sigma.BoilerMng]^{\mathtt{s}}_{loc2} \\
\rightarrowtriangle_{\mathrm{i}} & n_P[\mathcal{I}_P \bowtie \sigma.BoilerCtrl \mid LightCtrl]^{\mathtt{m}}_{l'} \;\big|\; n_B[\mathcal{I}_B'[boiler \mapsto \mathsf{on}] \bowtie \sigma.BoilerMng]^{\mathtt{s}}_{loc2} \\
= & n_P[\mathcal{I}_P \bowtie \sigma.BoilerCtrl \mid LightCtrl]^{\mathtt{m}}_{l'} \;\big|\; n_B[\mathcal{I}_B'' \bowtie \sigma.BoilerMng]^{\mathtt{s}}_{loc2}
\end{array}$$

where $\mathscr{I}''_B(temp) = t < \Theta$ and $\mathscr{I}''_B(boiler) = \mathsf{on}$. Now, both the phone and the boiler manager can only perform a timed reduction. However, the whole system may have further instantaneous reductions depending whether the phone is in position to interact with the light managers of the house. In any case, thanks to *well-timedness* (Proposition 4) and *patience* (Proposition 3) we will eventually have a reduction sequence of the form:

$$Sys'[temp \mapsto t] \;\rightarrowtriangle_{\mathrm{i}}^{*} \rightarrowtriangle_{\sigma}\; Phone'' \mid LR'_1 \mid LR'_2 \mid n_B[\mathscr{I}''_B \bowtie BoilerMng]^{\mathsf{s}}_{loc2}$$

where $\mathscr{I}''_B(temp) = t$, $\mathscr{I}''_B(boiler) = \mathsf{on}$, and the mobile phone may have moved to a new location l'', with $\mathrm{d}(l', l'') = 1$.

3. Let us consider the evolution of $Sys'[temp \mapsto t]$, with $t \geq \Theta$. Here, similarly to the previous case, we can derive:

$$\begin{array}{rcl} Sys'[temp \mapsto t] & \equiv & Phone' \mid LR_1 \mid LR_2 \mid n_B[\mathscr{I}_B[temp \mapsto t] \bowtie BoilerMng]^{\mathsf{s}}_{loc2} \\ & \rightarrowtriangle_{\mathrm{i}}^{*} \rightarrowtriangle_{\sigma} & Phone'' \mid LR'_1 \mid LR'_2 \mid n_B[\mathscr{I}'_B \bowtie BoilerMng]^{\mathsf{s}}_{loc2} \end{array}$$

with $\mathscr{I}'_B(temp) = t$ and $\mathscr{I}'_B(boiler) = \mathsf{off}$.

4. We prove only the implication from left to right. The other is similar. We know that $Sys' \rightarrowtriangle_{\mathrm{i}}^{*} Sys'' \downarrow_{light_1!\mathsf{on}}$. By Lemma 9 we know the structure of Sys'. We recall that in Sys the actuator $light_1$ is set to off. Notice also that this actuator is exclusively managed via the process $LightMng_1$, running at the stationary node n_1, located al $loc1$. More precisely, the actuator $light_1$ can be modified by $LightMng_1$ only after a synchronisation at the short-range channel c_1. We recall that $\mathrm{rng}(c_1) = 0$. We also recall that mobile nodes can change their location only by executing a timed reduction via rule (timemob). We fixed $\delta = 1$, which is the maximum distance that a mobile node can afford within a time unit. Thus, if $Sys' \rightarrowtriangle_{\mathrm{i}}^{*} Sys'' \downarrow_{light_1!\mathsf{on}}$ there are two possibilities:
   - either the mobile phone is current time interval is located at $loc1$;
   - or the mobile phone was located at $loc1$ in the previous time interval, and in the current time interval it is in a location l', with $\mathrm{d}(l', loc_1) = 1$, as $\delta = 1$.

   In the first case, the light manager $LightMng_2$, located at $loc4$, has necessarily set the actuator $light_2$ to off. This is because $\mathrm{rng}(c_2) = 0$, $\mathrm{d}(loc1, loc4) = 3$, and the only manner to switch on $light_2$ is to place the mobile phone at $loc4$. However, as the mobile phone is currently at $loc1$, and $\delta = 1$, this could have happened only 3 time instants ago. By that time, the timemout in $LightMng_2$ has already switched off the light.

   The second case, when the mobile phone is currently located at some location l', with $\mathrm{d}(l', loc_1) = 1$, is similar. This is because $\mathrm{d}(loc1, loc4) = 3$, and by triangular inequality $\mathrm{d}(l', loc4) \geq 2$. Thus, the phone is far enough to ensure that timeout of $LightMng_2$ already fired to switch off $light_2$.

□

A.3 Proofs of Section 4

This section is devoted to the proof of the *Harmony Theorem* (Theorem 1). We start with a technical lemma that provides the structure of a process depending on its possible actions.

Lemma 10. *Let P be a process.*

1. *If* $P \xrightarrow{\sigma} P'$ *then* $P \equiv \prod_{i \in I} \lfloor \pi_i.P_i \rfloor Q_i \mid \prod_{j \in J} \sigma.P_j$ *and* $P' \equiv \prod_{i \in I} Q_i \mid \prod_{j \in J} P_j$*, for appropriate index sets, prefixes and processes*
2. *If* $P \xrightarrow{s?v} P'$ *then there are* P_1 *and* Q *such that* $P \equiv s?(x).P_1 \mid Q$ *and* $P' \equiv P_1\{^{v}/_{x}\} \mid Q$

3. *If $P \xrightarrow{a!v} P'$ then there are P_1 and Q such that $P \equiv a!v.P_1 \mid Q$ and $P' \equiv P_1 \mid Q$*
4. *If $P \xrightarrow{@h} P'$ then there are P_1 and Q such that $P \equiv @(x).P_1 \mid Q$ and $P' \equiv P_1\{{}^{h}\!/_{x}\} \mid Q$*
5. *If $P \xrightarrow{\bar{c}v} P'$ then there are P_1, Q_1 and Q such that $P \equiv \lfloor \bar{c}\langle v\rangle.P_1 \rfloor Q_1 \mid Q$ and $P' \equiv P_1 \mid Q$*
6. *If $P \xrightarrow{cv} P'$, then there exist P_1, Q_1, Q s.t. $P \equiv \lfloor c(x).P_1 \rfloor Q_1 \mid Q$ and $P' \equiv P_1\{{}^{v}\!/_{x}\} \mid Q$*
7. *If $P \xrightarrow{\tau} P'$ then there are P_1, P_2, Q_1, Q_2, R, and c with $\mathrm{rng}(c) = -1$, such that $P \equiv \lfloor c(x).P_1 \rfloor Q_1 \mid \lfloor \bar{c}\langle v\rangle.P_2 \rfloor Q_2 \mid R$ and $P' \equiv P_1\{{}^{v}\!/_{x}\} \mid P_2 \mid R$.*

Proof. Let us start with item (1). We proceed by rule induction on why $P \xrightarrow{\sigma} P'$.

- Let $P \xrightarrow{\sigma} P'$ by an application of rule (TimeNil); then the result is immediate for $I = J = \emptyset$.
- Let $P \xrightarrow{\sigma} P'$ by an application of rule (Delay) with $P = \sigma.P_1$ and $P' = P_1$. Thus, for $I = \emptyset$ and $J = \{1\}$ we have $P = \sigma.P_1 \equiv \mathsf{nil} \mid \sigma.P_1$ and $P' = P_1 \equiv \mathsf{nil} \mid P_1$.
- Let $P \xrightarrow{\sigma} P'$ by an application of rule (Timeout) with $P = \lfloor \pi_1.P_1 \rfloor Q_1$ and $P' = Q_1$. Thus, for $I = \{1\}$ and $J = \emptyset$ we have $P = \lfloor \pi_1.P_1 \rfloor Q_1 \equiv \lfloor \pi_1.P_1 \rfloor Q_1 \mid \mathsf{nil}$ and $P' = Q_1 \equiv Q_1 \mid \mathsf{nil}$.
- Let $P \xrightarrow{\sigma} P'$ by an application of rule (TimeParP) with $P = R_1 \mid R_2$ and $P' = R_1' \mid R_2'$, because $R_1 \xrightarrow{\sigma} R_1'$ and $R_2 \xrightarrow{\sigma} R_2'$. By inductive hypothesis, there exist I, J, I' and J' such that $R_1 \equiv \prod_{i\in I} \lfloor \pi_i.P_i \rfloor Q_i \mid \prod_{j \in J} \sigma.P_j$, $R_1' \equiv \prod_{i\in I} Q_i \mid \prod_{j\in J} P_j$, $R_2 \equiv \prod_{i'\in I'} \lfloor \pi_{i'}.P_{i'} \rfloor Q_{i'} \mid \prod_{j'\in J'} \sigma.P_{j'}$ and $R_2' \equiv \prod_{i'\in I'} Q_{i'} \mid \prod_{j'\in J'} P_{j'}$. To conclude this case we choose as index sets $\bar{I} = I \cup I'$ and $\bar{J} = J \cup J'$.
- Let $P \xrightarrow{\sigma} P'$ by an application of rule (Fix) with $P = \mathsf{fix}X.P_1$ and $P' = P_2$, because $P_1\{{}^{\mathsf{fix}X.P_1}\!/_{X}\} \xrightarrow{\sigma} P_2$. By inductive hypothesis, there exist I and J such that $P_1\{{}^{\mathsf{fix}X.P_1}\!/_{X}\} \equiv \prod_{i\in I} \lfloor \pi_i.P_i \rfloor Q_i \mid \prod_{j\in J} \sigma.P_j$ and $P_2 \equiv \prod_{i\in I} Q_i \mid \prod_{j\in J} P_j$. By structural congruence we have $\mathsf{fix}X.P_1 \equiv P_1\{{}^{\mathsf{fix}X.P_1}\!/_{X}\}$ and therefore $P = \mathsf{fix}X.P_1 \equiv \prod_{i\in I} \lfloor \pi_i.P_i \rfloor Q_i \mid \prod_{j\in J} \sigma.P_j$.

Let us prove the item (2) of the proposition. We proceed by rule induction on why $P \xrightarrow{s?v} P'$.

- Let $P \xrightarrow{s?v} P'$ by an application of rule (Sensor) with $P = s?(x).P_1$ and $P' = P_1\{{}^{v}\!/_{x}\}$. This case is easy.
- Let $P \xrightarrow{s?v} P'$ by an application of rule (Fix) with $P = \mathsf{fix}X.P_1$ and $P' = P_2$, because $P_1\{{}^{\mathsf{fix}X.P_1}\!/_{X}\} \xrightarrow{s?v} P_2$. By inductive hypothesis there exist P_3 and Q_1 such that $P_1\{{}^{\mathsf{fix}X.P_1}\!/_{X}\} \equiv s?(x).P_3 \mid Q_1$ and $P_2 \equiv P_3\{{}^{v}\!/_{x}\} \mid Q_1$. By structural congruence $P = \mathsf{fix}X.P_1 \equiv P_1\{{}^{\mathsf{fix}X.P_1}\!/_{X}\} \equiv s?(x).P_3 \mid Q_1$.
- Let $P \xrightarrow{s?v} P'$ by an application of rule (ParP) with $P = P_1 \mid R$ and $P' = P_1' \mid R$, because $P_1 \xrightarrow{s?v} P_1'$. By inductive hypothesis there exist P_2 and Q_1 such that $P_1 \equiv s?(x).P_2 \mid Q_1$ and $P_1' \equiv P_2\{{}^{v}\!/_{x}\} \mid Q_1$, thus, the thesis holds for $Q = Q_1 \mid R$.

The cases (3), (4), (5) and (6) are analogous to previous items. We prove (7). We proceed by rule induction on why $P \xrightarrow{\tau} P'$.

- Let $P \xrightarrow{\tau} P'$ by an application of rule (Com). Then our result follows by application of the items (5) and (6) of the proposition. We need to work up to structural congruence.
- Let $P \xrightarrow{\tau} P'$ by an application of rule (ParP) or (Fix). This case is analogous to that the corresponding ones in (2).

□

Lemma 11.

1. *If $M \xrightarrow{\bar{c}v@h} M'$ then $M \equiv (\nu\tilde{g})\big(n[\mathscr{I} \bowtie \lfloor \bar{c}\langle v\rangle.P \rfloor P' \mid Q]^{\mu}_{h} \mid N\big)$ and $M' \equiv (\nu\tilde{g})\big(n[\mathscr{I} \bowtie P \mid Q]^{\mu}_{h} \mid N\big)$, for some $n, P, P', Q, \mu, N, \tilde{g}$, with $c \notin \tilde{g}$.*

2. *If $M \xrightarrow{cv@h} M'$ then $M \equiv (\nu\tilde{g})\big(n[\mathscr{I} \bowtie \lfloor c(x).P \rfloor P' \mid Q]^{\mu}_{h} \mid N\big)$ and $M' \equiv (\nu\tilde{g})\big(n[\mathscr{I} \bowtie P\{^{v}/_{x}\} \mid Q]^{\mu}_{h} \mid N\big)$, for some $n, P, P', Q, \mu, N, \tilde{g}$, with $c \notin \tilde{g}$.*

Proof. We start with the proof of item (1). We proceed by rule induction.

- Let $M \xrightarrow{\bar{c}v@k} M'$ by an application of rule rule (SndN) because $P \xrightarrow{\bar{c}v} P'$ and $\mathrm{rng}(c) \geq 0$, with $M = n[\mathscr{I} \bowtie P]^{\mu}_{k}$ and $M' = n[\mathscr{I} \bowtie P']^{\mu}_{k}$. Lemma 10(5) ensures that since $P \xrightarrow{\bar{c}v} P'$ then there exist P_1, Q_1, Q such that $P \equiv \lfloor \bar{c}\langle v \rangle.P_1 \rfloor Q_1 \mid Q$ and $P' \equiv P_1 \mid Q$. This implies $M \equiv n[\mathscr{I} \bowtie \lfloor \bar{c}\langle v \rangle.P_1 \rfloor Q_1 \mid Q]^{\mu}_{k}$ and $M' \equiv n[\mathscr{I} \bowtie P_1 \mid Q]^{\mu}_{k}$.
- Let $M \xrightarrow{\bar{c}v@k} M'$ by an application of rule (ParN) because $M_1 \xrightarrow{\bar{c}v@k} M_1'$, with $M = M_1 \mid M_2$ and $M' = M_1' \mid M_2$. By inductive hypothesis, since $M_1 \xrightarrow{\bar{c}v@k} M_1'$, there exist $n, P_1, P_1', Q_1, \mu, k, N_1, \tilde{g}$ such that $c \notin \tilde{g}$ and $M_1 \equiv (\nu\tilde{g})n[\mathscr{I} \bowtie \lfloor \bar{c}\langle v \rangle P_1 \rfloor P_1' \mid Q_1]^{\mu}_{k} \mid N_1$ and $M_1' \equiv (\nu\tilde{g})n[\mathscr{I} \bowtie P_1 \mid Q_1]^{\mu}_{k} \mid N_1$. Hence $M \equiv (\nu\tilde{g})n[\mathscr{I} \bowtie \lfloor \bar{c}\langle v \rangle P_1 \rfloor P_1' \mid Q_1]^{\mu}_{k} \mid N_1 \mid M_2$ and the system M' is such that $M' \equiv (\nu\tilde{g})n[\mathscr{I} \bowtie P_1 \mid Q_1]^{\mu}_{k} \mid N_1 \mid M_2$. This concludes the case, for $N = N_1 \mid M_2$.
- Let $M \xrightarrow{\bar{c}v@k} M'$ by an application of rule (Res) because $M_1 \xrightarrow{\bar{c}v@k} M_1'$, with $c \neq c'$, $M = (\nu c')M_1$ and $M' = (\nu c')M_1'$. By inductive hypothesis, there exist $n, P_1, P_1', Q_1, \mu, k, N_1, \tilde{g}$ such that $c \notin \tilde{g}$ and $M_1 \equiv (\nu\tilde{g})n[\mathscr{I} \bowtie \lfloor \bar{c}\langle v \rangle P_1 \rfloor P_1' \mid Q_1]^{\mu}_{k} \mid N_1$ and $M_1' \equiv (\nu\tilde{g})n[\mathscr{I} \bowtie P_1 \mid Q_1]^{\mu}_{k} \mid N_1$. Hence $M \equiv (\nu c')(\nu\tilde{g})n[\mathscr{I} \bowtie \lfloor \bar{c}\langle v \rangle P_1 \rfloor P_1' \mid Q_1]^{\mu}_{k} \mid N_1$ and $M' \equiv (\nu c')(\nu\tilde{g})n[\mathscr{I} \bowtie P_1 \mid Q_1]^{\mu}_{k} \mid N_1$. Thus, since $c \notin (\nu c')(\nu\tilde{g})$ this concludes the case.

The remaining item (2) is analogous by applying Lemma 10(6). □

Lemma 12. *If $M \xrightarrow{\alpha} M'$ and $M \equiv N$ then there is N' such that $N \xrightarrow{\alpha} N'$ and $M' \equiv N'$.*

Proof of Theorem 1

Proof. We have to prove the following sub-results:

1. If $M \xrightarrow{\tau} M'$ then $M \mathrel{-\!\!\triangleright}_{\tau} M'$
2. If $M \mathrel{-\!\!\triangleright}_{\tau} M'$ then $M \xrightarrow{\tau}\equiv M'$
3. If $M \xrightarrow{a} M'$ then $M \mathrel{-\!\!\triangleright}_{a} M'$
4. If $M \mathrel{-\!\!\triangleright}_{a} M'$ then $M \xrightarrow{a} \equiv M'$
5. If $M \xrightarrow{\sigma} M'$ then $M \mathrel{-\!\!\triangleright}_{\sigma} M'$
6. If $M \mathrel{-\!\!\triangleright}_{\sigma} M'$ then $M \xrightarrow{\sigma} \equiv M'$.

Let us start with the sub-result (1). The proof is by rule induction on why $M \xrightarrow{\tau} M'$.

- Let $M \xrightarrow{\tau} M'$ by an application of rule (SensRead), with $M = n[\mathscr{I} \bowtie P]^{\mu}_{h}$ and $M' = n[\mathscr{I} \bowtie P']^{\mu}_{h}$, because $\mathscr{I}(s) = v$ and $P \xrightarrow{s?v} P'$. By Lemma 10(2) there exist P_1, Q such that $P \equiv s?(x).P_1 \mid Q$ and $P' \equiv P_1\{^{v}/_{x}\} \mid Q$. Then we can apply the reduction rules (sensread) and (parp) to infer $M \mathrel{-\!\!\triangleright}_{\tau} M'$, as required.
- Let $M \xrightarrow{\tau} M'$ by an application of rule (Pos). This case follows by an application of Lemma 10(4) together with reduction rules (pos) and (parp).
- Let $M \xrightarrow{\tau} M'$ by an application of rule (LocCom), with $M = n[\mathscr{I} \bowtie P]^{\mu}_{k}$ and $M' = n[\mathscr{I} \bowtie P']^{\mu}_{k}$, because $P \xrightarrow{\tau} P'$. By Lemma 10(7), $P \xrightarrow{\tau} P'$ ensures that there exist P_1, P_2, Q_1, Q_2, R, c with $\mathrm{rng}(c) = -1$ such that $P \equiv \lfloor c(x).P_1 \rfloor Q_1 \mid \lfloor \bar{c}\langle v \rangle.P_2 \rfloor Q_2 \mid R$ and $P' \equiv P_1\{^{v}/_{x}\} \mid P_2 \mid R$. By structural congruence we have $M \equiv n[\mathscr{I} \bowtie \lfloor c(x).P_1 \rfloor Q_1 \mid \lfloor \bar{c}\langle v \rangle.P_2 \rfloor Q_2 \mid R]^{\mu}_{k}$ and analogously $M' \equiv n[\mathscr{I} \bowtie P_1\{^{v}/_{x}\} \mid P_2 \mid R]^{\mu}_{k}$. Hence, by an application of rules (struct) and (loccom) we can infer $M \mathrel{-\!\!\triangleright}_{\tau} M'$.

- Let $M \xrightarrow{\tau} M'$ by an application of rule (ActUnChg). This case follows by an application of Lemma 10(3) together with an application of reduction rules (actunchg) and (parp).
- Let $M \xrightarrow{\tau} M'$ by an application of rule (ParN), with $M = M_1 \mid M_2$ and $M' = M_1' \mid M_2$, because $M_1 \xrightarrow{\tau} M_1'$. By inductive hypothesis $M_1 \rightarrowtriangle_{\tau} M_1'$. Therefore, by an application of rule (parn) we can infer $M \rightarrowtriangle_{\tau} M'$.
- Let $M \xrightarrow{\tau} M'$ by an application of rule (Res), with $M = (\nu\tilde{g})M_1$ and $M' = (\nu\tilde{g})M_1'$, because $M_1 \xrightarrow{\tau} M_1'$. By inductive hypothesis $M_1 \rightarrowtriangle_{\tau} M_1'$. Therefore, by an application of the reduction rule (res) we derive $M \rightarrowtriangle_{\tau} M'$.
- Let $M \xrightarrow{\tau} M'$ by an application of rule (GlbCom), with $M = M_1 \mid M_2$ and $M' = M_1' \mid M_2'$, because $M_1 \xrightarrow{\bar{c}v@h} M_1'$ and $M_2 \xrightarrow{cv@k} M_2'$ and $\mathsf{d}(h,k) \leq \mathrm{rng}(c)$. Since $M_1 \xrightarrow{\bar{c}v@h} M_1'$, Lemma 11(1) guarantees that $M_1 \equiv (\nu\tilde{g})n[\mathscr{I} \bowtie \lfloor \bar{c}\langle v\rangle P \rfloor P' \mid R]_h^{\mu} \mid N$ and $M_1' \equiv (\nu\tilde{g})n[\mathscr{I} \bowtie P \mid R]_h^{\mu} \mid N$, for some $n, P, P', R, \mu, h, N, \tilde{g}$. Furthermore, by Lemma 11(2) there exist m, Q, Q', $R', \mu, k, N', \tilde{g}'$ such that $M_2 \equiv (\nu\tilde{g}')m[\mathscr{I} \bowtie \lfloor c(x)Q \rfloor Q' \mid R']_k^{\mu} \mid N'$ and $M_2' \equiv (\nu\tilde{g}')m[\mathscr{I} \bowtie Q\{^{v}\!/_{x}\} \mid R']_k^{\mu} \mid N'$. Therefore, by applying the reduction rules (struct), (res), (glbcom), (parp) and (parn) we can infer $M \rightarrowtriangle_{\tau} M'$.

Let us prove the sub-result (2) by rule induction on why $M \rightarrowtriangle_{\tau} M'$.

- Let $M \rightarrowtriangle_{\tau} M'$ by rule (sensread), with $M = n[\mathscr{I} \bowtie s?(x).P \mid Q]_h^{\mu}$ and $M' = n[\mathscr{I} \bowtie P\{^{v}\!/_{x}\} \mid Q]_h^{\mu}$, because $\mathscr{I}(s) = v$. Hence, by rule (Sensor) we have $s?(x).P \xrightarrow{s?v} P\{^{v}\!/_{x}\}$, by rule (ParP) we have $s?(x).P \mid Q \xrightarrow{s?v} P\{^{v}\!/_{x}\} \mid Q$ and finally by rule(SensRead) we have $n[\mathscr{I} \bowtie s?(x).P \mid Q]_h^{\mu} \xrightarrow{\tau} n[\mathscr{I} \bowtie P\{^{v}\!/_{x}\} \mid Q]_h^{\mu}$.
- Let $M \rightarrowtriangle_{\tau} M'$ by applying rule (pos), with $M = n[\mathscr{I} \bowtie @(x).P \mid Q]_h^{\mu}$ and $M' = n[\mathscr{I} \bowtie P\{^{x}\!/_{h}\} \mid Q]_h^{\mu}$. We get $M \xrightarrow{\tau}\equiv M'$ by applying rules (PosP), (ParP) and (Pos).
- Let $M \rightarrowtriangle_{\tau} M'$ by an application of rule (actunchg). This case is similar to the previous one, by an application of the transition rule (ActUnChg).
- Let $M \rightarrowtriangle_{\tau} M'$ by an application of rule (parp):
$$\frac{\prod_i n_i[\mathscr{I}_i \bowtie P_i]_{h_i}^{\mu_i} \rightarrowtriangle_{\tau} \prod_i n_i[\mathscr{I}_i' \bowtie P_i']_{h_i'}^{\mu_i}}{\prod_i n_i[\mathscr{I}_i \bowtie P_i \mid Q_i]_{h_i}^{\mu_i} \rightarrowtriangle_{\tau} \prod_i n_i[\mathscr{I}_i' \bowtie P_i' \mid Q_i]_{h_i'}^{\mu_i}}$$
By inductive hypothesis we have: $\prod_i n_i[\mathscr{I}_i \bowtie P_i]_{h_i}^{\mu_i} \xrightarrow{\tau}\equiv \prod_i n_i[\mathscr{I}_i' \bowtie P_i']_{h_i'}^{\mu_i}$. The τ-transition can be derived using different transition rules. Suppose that $\prod_i n_i[\mathscr{I}_i \bowtie P_i]_{h_i}^{\mu_i} \xrightarrow{\tau}\equiv \prod_i n_i[\mathscr{I}_i' \bowtie P_i']_{h_i'}^{\mu_i}$ by an application of rule (SensRead) to node n_j, for some $j \in I$. Then, by using rule (ParP) to derive $P_j \mid Q_j \xrightarrow{s?v} P_j' \mid Q_j$, rule (SensRead) to derive $n_j[\mathscr{I}_j \bowtie P_j \mid Q_j]_{h_j}^{\mu_j} \xrightarrow{\tau}\equiv n_j[\mathscr{I}_j' \bowtie P_j' \mid Q_j]_{h_j'}^{\mu_j}$, and rule (ParN) to derive $\prod_i n_i[\mathscr{I}_i \bowtie P_i \mid Q_i]_{h_i}^{\mu_i} \xrightarrow{\tau}\equiv \prod_i n_i[\mathscr{I}_i' \bowtie P_i' \mid Q_i]_{h_i'}^{\mu_i}$, we get $M \xrightarrow{\tau}\equiv M'$.
The cases when the τ-transition is derived by an application of the rules (ActUnChg), (Com) and (Pos) are similar.
- Let $M \rightarrowtriangle_{\tau} M'$ by an application of (loccom), with $M = n[\mathscr{I} \bowtie \lfloor \bar{c}\langle v\rangle.P \rfloor R \mid \lfloor c(x).Q \rfloor S]_h^{\mu}$ and $M' = n[\mathscr{I} \bowtie P \mid Q\{^{v}\!/_{x}\}]_h^{\mu}$, because $\mathrm{rng}(c) = -1$. Hence, for $\mathrm{rng}(c) = -1$ we can derive:
$$\frac{\dfrac{\lfloor \bar{c}\langle v\rangle.P \rfloor R \xrightarrow{\bar{c}v} P \qquad \lfloor c(v).Q \rfloor S \xrightarrow{cv} Q}{\lfloor \bar{c}\langle v\rangle.P \rfloor R \mid \lfloor c(x).Q \rfloor S \xrightarrow{\tau} P \mid Q\{^{v}\!/_{x}\}}}{n[\mathscr{I} \bowtie \lfloor \bar{c}\langle v\rangle.P \rfloor R \mid \lfloor c(x).Q \rfloor S]_h^{\mu} \xrightarrow{\tau} n[\mathscr{I} \bowtie P \mid Q\{^{v}\!/_{x}\}]_h^{\mu}}$$
and $M \xrightarrow{\tau}\equiv M'$ is derived as required.

- Let $M \mathrel{-\!\!\triangleright}_{\tau} M'$ by an application of (glbcom), with $M = n[\mathscr{I} \bowtie \lfloor \bar{c}\langle v\rangle.P\rfloor R]^{\mu}_{h} \mid m[\mathscr{I} \bowtie \lfloor c(x).Q\rfloor S]^{\mu'}_{k}$ and $M' = n[\mathscr{I} \bowtie P]^{\mu}_{h} \mid m[\mathscr{I} \bowtie Q\{^{v}/_{x}\}]^{\mu'}_{k}$, because $\mathrm{d}(h,k) \le \mathrm{rng}(c)$. Therefore the following derivation can be built up for $\mathrm{d}(h,k) \le \mathrm{rng}(c)$:

$$\dfrac{\dfrac{\lfloor \bar{c}\langle v\rangle.P\rfloor R \xrightarrow{\bar{c}v} P}{n[\mathscr{I} \bowtie \lfloor \bar{c}\langle v\rangle.P\rfloor R]^{\mu}_{h} \xrightarrow{\bar{c}v@h} n[\mathscr{I} \bowtie P]^{\mu}_{h}} \qquad \dfrac{\lfloor c(v).Q\rfloor S \xrightarrow{cv} Q}{m[\mathscr{I} \bowtie \lfloor c(v).Q\rfloor S]^{\mu'}_{k} \xrightarrow{cv@k} m[\mathscr{I} \bowtie Q\{^{v}/_{x}\}]^{\mu'}_{k}}}{n[\mathscr{I} \bowtie \lfloor \bar{c}\langle v\rangle.P\rfloor R]^{\mu}_{h} \mid m[\mathscr{I} \bowtie \lfloor c(x).Q\rfloor S]^{\mu'}_{k} \xrightarrow{\tau} n[\mathscr{I} \bowtie P]^{\mu}_{h} \mid m[\mathscr{I} \bowtie Q\{^{v}/_{x}\}]^{\mu'}_{k}}$$

  and we get $M \xrightarrow{\tau}\equiv M'$.
- Let $M \mathrel{-\!\!\triangleright}_{\tau} M'$ by an application of rule (res), with $M = (\nu\tilde{g})M_1$ and $M' = (\nu\tilde{g})M'_1$, because $M_1 \mathrel{-\!\!\triangleright}_{\tau} M'_1$. By inductive hypothesis we have $M_1 \xrightarrow{\tau}\equiv M'_1$. Hence, by applying transition rules (Res), we can derive $M \xrightarrow{\tau}\equiv M'$.
- Let $M \mathrel{-\!\!\triangleright}_{\tau} M'$ by an application of rule (struct) because $M \equiv N$, $N \mathrel{-\!\!\triangleright}_{\tau} N'$ and $N' \equiv M'$. By inductive hypothesis we have $N \xrightarrow{\tau}\equiv N'$. Since $M \equiv N$ and $M' \equiv N'$, by an application of Lemma 12 we obtain $M \xrightarrow{\tau}\equiv M'$.
- Let $M \mathrel{-\!\!\triangleright}_{\tau} M'$ by an application of rule (parn), with $M = M_1 \mid N$ and $M' = M'_1 \mid N$, because $M_1 \mathrel{-\!\!\triangleright}_{\tau} M'_1$. By inductive hypothesis $M_1 \mathrel{-\!\!\triangleright}_{\tau} M'_1$ implies that $M_1 \xrightarrow{\tau}\equiv M'_1$. Hence, an application of the transition rule (ParN) concludes this case.

Let us prove the sub-result (3). The proof is by rule induction on why $M \xrightarrow{a} M'$.

- Let $M \xrightarrow{a} M'$ by an application of rule (ActChg), with $M = n[\mathscr{I} \bowtie P]^{\mu}_{h}$ and $M' = n[\mathscr{I}' \bowtie P']^{\mu}_{h}$, because $\mathscr{I}(a) = w \neq v$, $P \xrightarrow{a!v} P'$ and $\mathscr{I}' := \mathscr{I}[a \mapsto v]$. By Lemma 10(3) there exist P_1, Q such that $P \equiv a!v.P_1 \mid Q$ and $P' \equiv P_1 \mid Q$. Then we can apply reduction rules (actchg) and (parp) to infer $M \mathrel{-\!\!\triangleright}_{a} M'$.
- The cases when $M \xrightarrow{a} M'$ is derived by an application of either rule (ParN) or rule (Res) are analogous to the corresponding cases when $M \xrightarrow{\tau} M'$.

Let us prove the sub-result (4). The proof is by rule induction on why $M \mathrel{-\!\!\triangleright}_{a} M'$.

- Let $M \mathrel{-\!\!\triangleright}_{a} M'$ by an application of rule (actchg), with $M = n[\mathscr{I} \bowtie a!v.P]^{\mu}_{h}$ and $M' = n[\mathscr{I}' \bowtie P]^{\mu}_{h}$, because $\mathscr{I}(a) = w \neq v$ and $\mathscr{I}' = \mathscr{I}[a \mapsto v]$. By an application of rule (Actuator) we derive $a!v.P \xrightarrow{a!v} P$. The thesis follows by an application of rule (ActChg).
- The cases when $M \mathrel{-\!\!\triangleright}_{a} M'$ is derived by an application of one of the rules among (parp), (parn), (res) or (struct) are analogous to the corresponding cases written for $M \mathrel{-\!\!\triangleright}_{\tau} M'$.

Let us prove the sub-result (5). The proof is by rule induction on why $M \xrightarrow{\sigma} M'$.

- Let $M \xrightarrow{\sigma} M'$ by an application of rule (TimeZero). This case is immediate.
- Let $M \xrightarrow{\sigma} M'$ by an application of rule (TimeStat), with $M = n[\mathscr{I} \bowtie P]^{\mathsf{s}}_{h}$ and $M' = n[\mathscr{I} \bowtie P']^{\mathsf{s}}_{h}$, because $P \xrightarrow{\sigma} P'$ and $n[\mathscr{I} \bowtie P]^{\mathsf{s}}_{h} \not\xrightarrow{\tau}$. Since $P \xrightarrow{\sigma} P'$, by Lemma 10(1) we derive $P \equiv \prod_{i\in I} \lfloor \pi_i.P_i \rfloor Q_i \mid \prod_{j\in J} \sigma.P_j$ and $P' \equiv \prod_{i\in I} Q_i \mid \prod_{j\in J} P_j$ for some $I, J, \pi_i, P_i, Q_i, P_j$. By an application of the sub-result (2) above, from $n[\mathscr{I} \bowtie P]^{\mathsf{s}}_{h} \not\xrightarrow{\tau}$ we derive $n[\mathscr{I} \bowtie P]^{\mathsf{s}}_{h} \not\mathrel{-\!\!\triangleright}_{\tau}$. Then the thesis follows by applying the reduction rule (timestat).
- Let $M \xrightarrow{\sigma} M'$ by an application of rule (TimeMob). This case is similar to the previous one by applying the reduction rule (timemob) in place of (timestat).
- Let $M \xrightarrow{\sigma} M'$ by an application of rule (TimePar), with $M = M_1 \mid M_2$ and $M' = M'_1 \mid M'_2$, because $M_1 \xrightarrow{\sigma} M'_1$, $M_2 \xrightarrow{\sigma} M'_2$ and $M_1 \mid M_2 \not\xrightarrow{\tau}$. By inductive hypothesis we have $M_1 \mathrel{-\!\!\triangleright}_{\sigma} M'_1$ and $M_2 \xrightarrow{\sigma}$

M_2'. Moreover, By an application of the sub-result (2) above $M_1 \mid M_2 \not\xrightarrow{\tau}$ implies $M_1 \mid M_2 \not\rightarrowtriangle_\tau$. Therefore we can apply the reduction rule (timepar) to get $M \rightarrowtriangle_\sigma M'$.

- Let $M \xrightarrow{\sigma} M'$ by an application of rule (Res). This case is similar to the corresponding one for $M \xrightarrow{\tau} M'$.

Let us prove the sub-result (6). The proof is by rule induction on why $M \rightarrowtriangle_\sigma M'$.

- Let $M \rightarrowtriangle_\sigma M'$ by an application of the reduction rule (timezero). This case is immediate.
- Let $M \rightarrowtriangle_\sigma M'$ by an application of rule (timestat):

$$\frac{n[\mathscr{I} \bowtie \prod_{i\in I}\lfloor \pi_i.P_i\rfloor Q_i \mid \prod_{j\in J}\sigma.P_j]^{\mathsf{s}}_h \not\rightarrowtriangle_\tau}{n[\mathscr{I} \bowtie \prod_{i\in I}\lfloor \pi_i.P_i\rfloor Q_i \mid \prod_{j\in J}\sigma.P_j]^{\mathsf{s}}_h \rightarrowtriangle_\sigma n[\mathscr{I} \bowtie \prod_{i\in I} Q_i \mid \prod_{j\in J} P_j]^{\mathsf{s}}_h}$$

  with $M = n[\mathscr{I} \bowtie \prod_{i\in I}\lfloor \pi_i.P_i\rfloor Q_i \mid \prod_{j\in J}\sigma.P_j]^{\mathsf{s}}_h$ and $M' = n[\mathscr{I} \bowtie \prod_{i\in I} Q_i \mid \prod_{j\in J} P_j]^{\mathsf{s}}_h$.
  By rule (Timeout) we derive $\lfloor \pi.P_i\rfloor Q_i \xrightarrow{\sigma} P_i$ and by rule (Delay) we derive $\sigma.P_j \xrightarrow{\sigma} P_j$. Now, we can repeatedly apply rule (TimeParP) to derive $\prod_{i\in I}\lfloor \pi_i.P_i\rfloor Q_i \mid \prod_{j\in J}\sigma.P_j \xrightarrow{\sigma} \prod_{i\in I} Q_i \mid \prod_{j\in J} P_j$. Indeed, by contradiction, if (TimeParP) would not be enabled, then rule (Com) would be enabled, and by applying rule (ParP), there would exist R such that $\prod_{i\in I}\lfloor \pi_i.P_i\rfloor Q_i \mid \prod_{j\in J}\sigma.P_j \xrightarrow{\tau} R$. Then, by applying rule (LocCom) and the sub-result (1) above, we would contradict the hypothesis $n[\mathscr{I} \bowtie \prod_{i\in I}\lfloor \pi_i.P_i\rfloor Q_i \mid \prod_{j\in J}\sigma.P_j]^{\mathsf{s}}_h \not\rightarrowtriangle_\tau$. Therefore, the thesis follows by applying the transition rule (TimeStat).
- Let $M \rightarrowtriangle_\sigma M'$ by an application of rule (timemob). This case is analogous to the previous one by applying the transition rule (TimeMob) in place of rule (TimeStat).
- Let $M \rightarrowtriangle_\sigma M'$ by an application of rule (timepar), with $M = M_1 \mid M_2$ and $M' = M_1' \mid M_2'$, because $M_1 \rightarrowtriangle_\sigma M_1'$, $M_2 \rightarrowtriangle_\sigma M_2'$, and $M_1 \mid M_2 \not\rightarrowtriangle_\tau$. By inductive hypothesis, $M_1 \rightarrowtriangle_\sigma M_1'$ implies $M_1 \xrightarrow{\sigma}_{\equiv} M_1'$ and $M_2 \rightarrowtriangle_\sigma M_2'$ implies $M_2 \xrightarrow{\sigma}\equiv M_2'$. Finally, by an an application of the sub-result (1) above $M_1 \mid M_2 \not\rightarrowtriangle_\tau$ implies $M_1 \mid M_2 \not\xrightarrow{\tau}$. Therefore we can derive $M \xrightarrow{\sigma}\equiv M'$ by an application of the transition rule (TimePar).
- The cases when $M \rightarrowtriangle_\sigma M'$ is derived by an application of one of the rules (res) or (struct) are analogous to the corresponding cases written for $M \rightarrowtriangle_\tau M'$.

□

A.4 Proofs of Section 5

Proof of Theorem 2

Proof. It remains to prove that the bisimilarity relation, $\approx$, is preserved by parallel composition and channel restriction.

Let us prove that $\approx$ is preserved by parallel composition. We show that the relation

$$\mathscr{R} = \{(M \mid O,\, N \mid O) : \text{ both } M \mid O \text{ and } N \mid O \text{ are well-formed and } M \approx N\}$$

is a bisimulation. We proceed by case analysis on why $M \mid O \xrightarrow{\alpha} \hat{M}$.

- Let $M \mid O \xrightarrow{\tau} \hat{M}$. We can distinguish two cases.
  - The transition is derived by applying rule (GlbCom), with $\hat{M} = M' \mid O'$, because $M \xrightarrow{\bar{c}v@h} M'$, $O \xrightarrow{cv@k} O'$, and $\mathrm{d}(h,k) \leq \mathrm{rng}(c)$. Since $M \xrightarrow{\bar{c}v@h} M'$ and $\mathrm{d}(h,k) \leq \mathrm{rng}(c)$, by an application of rule (SndObs) we derive $M \xrightarrow{\bar{c}v\triangleright k} M'$. As $M \approx N$, there are N_1, N_2 and N' such that $N \Longrightarrow$

$N_1 \xrightarrow{\bar{c}v\triangleright k} N_2 \Longrightarrow N'$ with $M' \approx N'$. Thus, there exists a location h' such that $\mathrm{d}(h',k) \leq \mathrm{rng}(c)$ and $N_1 \xrightarrow{\bar{c}v@h'} N_2$. Therefore, by several applications of rule (ParN) and one application of rule (GlbCom) we can derive $N \mid O \Rightarrow \hat{N} = N' \mid O'$, with $(\hat{M},\hat{N}) \in \mathscr{R}$. The symmetric case is analogous.

  - The transition is derived by applying rule (ParN) because $M \xrightarrow{\tau} M'$. As $M \approx N$ it follows that $N \Longrightarrow N'$ with $M' \approx N'$. By several applications of rule (ParN) it follows that $N \mid O \Rightarrow \hat{N} = N' \mid O'$, with $(\hat{M},\hat{N}) \in \mathscr{R}$. The symmetric case is easier.

- Let $M \mid O \xrightarrow{\sigma} \hat{M} = M' \mid O'$. This is only possible by an application of of rule (TimePar) because $M \xrightarrow{\sigma} M'$, $O \xrightarrow{\sigma} O'$ and $M \mid O \not\xrightarrow{\tau}$. Since $M \approx N$ and $M \xrightarrow{\sigma} M'$ there are N_1, N_2 and N' such that $N \Rightarrow N_1 \xrightarrow{\sigma} N_2 \Rightarrow N'$, with $M' \approx N'$. By an appropriate number of applications of rule (ParN) we have that $N \mid O \Rightarrow N_1 \mid O$. Next step is to show that we can use rule (TimePar) to derive $N_1 \mid O \xrightarrow{\sigma} N_2 \mid O'$. For that we only need to prove that $N_1 \mid O \not\xrightarrow{\tau}$. In fact, if $N_1 \mid O \xrightarrow{\tau}$ then we would reach a contradiction. This because, $M \approx N$ and $N \Rightarrow N_1$ implies there is M_1 such that $M \Rightarrow M_1$ with $M_1 \approx N_1$. As $M \not\xrightarrow{\tau}$ it follows that $M = M_1 \approx N_1$. By Proposition 2, $N_1 \xrightarrow{\sigma} N_2$ and $O \xrightarrow{\sigma} O'$ imply $N_1 \not\xrightarrow{\tau}$ and $O \not\xrightarrow{\tau}$. Thus $N_1 \mid O \xrightarrow{\tau}$ could be derived only by an application of rule (GlobCom) where N_1 interact with O via some channel c, with $\mathrm{rng}(c) \geq 0$. However, as $N_1 \approx M$ the network M could mimic the same interaction with O giving rise to a reduction of the form $M \mid O \Rightarrow\xrightarrow{\tau}$. This is in contradiction with the initial hypothesis that $M \mid O \not\xrightarrow{\tau}$. Thus, $N_1 \mid O \not\xrightarrow{\tau}$ and by an application of rule (TimePar) we derive $N_1 \mid O \xrightarrow{\sigma} N_2 \mid O'$. By an appropriate number of applications of rule (ParN) we get $N_2 \mid O' \Rightarrow N' \mid O'$. Thus, $N \mid O \xRightarrow{\sigma} \hat{N} = N' \mid O'$, with $(\hat{M},\hat{N}) \in \mathscr{R}$.
- Let $M \mid O \xrightarrow{a} \hat{M}$. Then, we distinguish two cases.
  - Either $O \xrightarrow{a} O'$ and by an application of rule (ParN) we derive $M \mid O \xrightarrow{a} M \mid O'$. This case is easy.
  - Or $M \xrightarrow{a} M'$ and by an application of rule (ParN) we derive $M \mid O \xrightarrow{a} M' \mid O$. As $M \approx N$ there is N' such that $N \xRightarrow{a} N'$ and $M' \approx N'$. Thus, by several applications of rule (ParN) we derive $N \mid O \xRightarrow{a} \hat{N} = N' \mid O$, with $(\hat{M},\hat{N}) \in \mathscr{R}$.
- Let $M \mid O \xrightarrow{\bar{c}v\triangleright k} \hat{M}$. By definition of rule (SndObs) this is only possible if $M \mid O \xrightarrow{\bar{c}v@h} \hat{M}$, with $\mathrm{d}(h,k) \leq \mathrm{rng}(c)$. Then, we distinguish two cases.
  - Either $O \xrightarrow{\bar{c}v@h} O'$ and $\hat{M} = M \mid O'$ by an application of rule (ParN). Then, by an application of the same rule we derive $N \mid O \xrightarrow{\bar{c}v@h} N \mid O'$. By an application of rule (SndObs) we get $N \mid O \xrightarrow{\bar{c}v\triangleright k} \hat{N} = N \mid O'$, with $(\hat{M},\hat{N}) \in \mathscr{R}$.
  - Or $M \xrightarrow{\bar{c}v@h} M'$ and $\hat{M} = M' \mid O$ by an application of rule (ParN). By an application of rule (SndObs) we have $M \xrightarrow{\bar{c}v\triangleright k} M'$. As $M \approx N$ there is N' such that $N \xRightarrow{\bar{c}v\triangleright k} N'$, with $M' \approx N'$. As the transition $\xrightarrow{\bar{c}v\triangleright k}$ can only be derived by an application of rule (SndObs), it follows that $N \xRightarrow{\bar{c}v@h'} N'$, for some h' such that $\mathrm{d}(h',k) \leq \mathrm{rng}(c)$. By several applications of rule (ParN) it follows that $N \mid O \xRightarrow{\bar{c}v@h'} N' \mid O$. By an application of rule (SndObs) we finally obtain $N \mid O \xRightarrow{\bar{c}v\triangleright k} \hat{N} = N' \mid O$, with $(\hat{M},\hat{N}) \in \mathscr{R}$.
- Let $M \mid O \xrightarrow{cv\triangleright k} \hat{M}$. This case is similar to the previous one.

Let us prove that $\approx$ is preserved by channel restriction. We show that the relation $\mathscr{R}$, defined as $\{\big((\nu c)M,\ (\nu c)N\big) : M \approx N\}$ is a bisimulation. We proceed by case analysis on why $(\nu c)M \xrightarrow{\alpha} \hat{M}$.

- Let $(\nu c)M \xrightarrow{\alpha} \hat{M}$, for $\alpha \in \{\tau, \sigma, a\}$. In this case, this transition has been derived by an application of rule (Res) because $M \xrightarrow{\alpha} M'$, with $\hat{M} = (\nu c)M'$. As $M \approx N$ there is N' such that $N \overset{\alpha}{\Longrightarrow} N'$ and $M' \approx N'$. By several applications of rule (Res) we can derive $(\nu c)N \overset{\alpha}{\Longrightarrow} \hat{N} = (\nu c)N'$, with $(\hat{M}, \hat{N}) \in \mathscr{R}$.
- Let $(\nu c)M \xrightarrow{\alpha} \hat{M}$, for $\alpha \in \{\overline{d}v \triangleright k, dv \triangleright k\}$, with $d \neq c$. This case is similar to the previous one except for the fact that we need to pass through the definitions of rules (SndObs) and (RcvObs) as the rule (Res) is only defined for intensional actions.
- Let $(\nu c)M \xrightarrow{\alpha} \hat{M}$, for $\alpha \in \{\overline{c}v \triangleright k, cv \triangleright k\}$. This case is not admissible as rule (Res) blocks intensional actions of the form $\overline{c}v@h$ and $cv@h$.

□

Next, we prove Lemma 2. For that we need a technical lemma.

Lemma 13. *Let $O = n[\mathscr{I} \bowtie \mathsf{nil}]^{\mathsf{s}}_k$ for an arbitrary node name n, an arbitrary actuator a, and an arbitrary value v in the domain of a, such that $\mathscr{I}$ is only defined for a and $\mathscr{I}(a) = v$. If $M \mid O \cong N \mid O$ then $M \cong N$.*

Proof. We recall that we always work with well-formed systems. The proofs consists in showing that the relation

$$\mathscr{R} = \{(M,N) : M \mid O \cong N \mid O, \text{ for some } O \text{ defined as above}\}.$$

is barb preserving, reduction closed and contextual. Since $\cong$ is the largest relation satisfying these properties, then $\mathscr{R} \subseteq \cong$ and therefore $M \cong N$. The scheme of the proof is very similar to that of the following proof. □

Proof of Lemma 2

Proof. Let $O = n[\mathscr{I} \bowtie a!v.\mathsf{nil}]^{\mathsf{s}}_k$, for an arbitrary node name n, an arbitrary actuator a, and arbitrary values v and w, in the domain of a, such that $\mathscr{I}$ is only defined for a and $\mathscr{I}(a) = w \neq v$. Let use define the relation

$$\mathscr{R} = \{(M,N) : M \mid O \cong N \mid O, \text{ for some } O \text{ defined as above}\} \ .$$

We show that the relation $\mathscr{R} \cup \cong$ is barb preserving, reduction closed and contextual. Since $\cong$ is the largest relation satisfying these properties, then $\mathscr{R} \subseteq \cong$ and therefore $M \cong N$.

We recall that in this paper we only consider well-formed networks. So, in the definition of $\mathscr{R}$ we assume that all systems of the form $M \mid O$ and $N \mid O$ are well-formed. In particular, in order to decide whether $(M,N) \in \mathscr{R}$ it is enough to find an O of the indicated shape, which respects the requirements of $\mathscr{R}$, and which preserves well-formedness.

Let us prove that $\mathscr{R} \cup \cong$ is barb-preserving. We concentrate on the relation $\mathscr{R}$. As O has neither channels or sensors it is basically isolated from the rest of the world, except for signals emitted on the actuator a. So, it is very easy to see that $\mathscr{R}$ is barb preserving from $M \mid O \cong N \mid O$.

Let us prove that $\mathscr{R} \cup \cong$ is reduction closed. We focus on $\mathscr{R}$. Recall that $\multimap \overset{\text{def}}{=} \multimap_\tau \cup \multimap_\sigma$. Let $(M,N) \in \mathscr{R}$ and $M \multimap_\tau M'$, for some M'. We have to show that $N \multimap^* N'$, for some N' such that $(M',N') \in \mathscr{R} \cup \cong$. Let us fix an O which respects the requirements of $\mathscr{R}$. By an application of rule (parn) we infer $M \mid O \multimap_\tau M' \mid O$. As $M \mid O \cong N \mid O$ there is $\overline{N}$ such that $N \mid O \multimap^* \overline{N}$ and $M' \mid O \cong \overline{N}$. Since O cannot communicate and since the only enabled reduction for O is $\multimap_a$, none of the reductions in the reduction sequence $N \mid O \multimap^* \overline{N}$ involves O and none of these reductions is a timed one. Therefore, $\overline{N} = N' \mid O$, $N \multimap_\tau^* N'$, and $M' \mid O \cong N' \mid O$. This implies $(M',N') \in \mathscr{R}$.

Let $(M,N) \in \mathscr{R}$ and $M \rightarrowtriangle_b M'$, for some M'. As both systems $M \mid O$ and $N \mid O$ are well-formed, the actuator a cannot appear neither in M or in N. Thus, $a \neq b$. Starting from $M \mid O \cong N \mid O$ we reason as in the previous case.

Let $(M,N) \in \mathscr{R}$ and $M \rightarrowtriangle_\sigma M'$, for some M'. We have to show that $N \rightarrowtriangle^* N''$, for some N'' such that $(M',N'') \in \mathscr{R} \cup \cong$. By definition of $\mathscr{R}$ we have $M \mid O \cong N \mid O$. Let $M \mid O \rightarrowtriangle_a M \mid n[\mathscr{I}[a \mapsto v] \bowtie \mathsf{nil}]^{\mathsf{s}}_{k}$, by an application of rules (actchg) and (parn). As $\cong$ is reduction closed it follows that there is $\overline{N}$ such that $N \mid O \rightarrowtriangle^* \rightarrowtriangle_a \rightarrowtriangle^* \overline{N}$, with $M \mid n[\mathscr{I}[a \mapsto v] \bowtie \mathsf{nil}]^{\mathsf{s}}_{k} \cong \overline{N}$. Due to the structure of O the last reduction sequence can be decomposed as follows: $N \mid O \rightarrowtriangle^* \rightarrowtriangle_a \rightarrowtriangle^* \overline{N} = N' \mid n[\mathscr{I}[a \mapsto v] \bowtie \mathsf{nil}]^{\mathsf{s}}_{k}$, for some N' such that $N \rightarrowtriangle^* N'$. Thus, for $O' = n[\mathscr{I}[a \mapsto v] \bowtie \mathsf{nil}]^{\mathsf{s}}_{k}$, we have $M \mid O' \cong N' \mid O'$. Since $M \rightarrowtriangle_\sigma M'$, by Proposition 2, there is no M'' such that $M \rightarrowtriangle_\tau M''$. More generally, by looking at the definition of O' it is easy to see that there is no U such that $M \mid O' \rightarrowtriangle_\tau U$. Thus, by an application of rules (timestat) and (timepar) we can infer $M \mid O' \rightarrowtriangle_\sigma M' \mid O'$. As $M \mid O' \cong N' \mid O'$, by Proposition 5 there is $\hat{N}$ such that $N' \mid O' \rightarrowtriangle_\tau^* \rightarrowtriangle_\sigma \rightarrowtriangle_\tau^* \hat{N}$ and $M' \mid O' \cong \hat{N}$. By looking at the definition of O' the only possibility is that $\hat{N} = N'' \mid O'$, with $N' \rightarrowtriangle_\tau^* \rightarrowtriangle_\sigma \rightarrowtriangle_\tau^* N''$ and $M' \mid O' \cong N'' \mid O'$. By Lem.13 this implies $M' \cong N''$. Recapitulating we have that for $M \rightarrowtriangle_\sigma M'$ there is N'' such that $N \rightarrowtriangle^* N''$, with $(M',N'') \in \mathscr{R} \cup \cong$.

Let us prove that $\mathscr{R} \cup \cong$ is contextual. Again, it is enough to focus on $\mathscr{R}$. Let us consider the three different network contexts:

- Let $(M,N) \in \mathscr{R}$. Let O' be an arbitrary network such that both $M \mid O'$ and $N \mid O'$ are well formed. We want to show that $(M \mid O' \,,\, N \mid O') \in \mathscr{R}$. As $(M,N) \in \mathscr{R}$, we can always find an $O = n[\mathscr{I} \bowtie a!v.\mathsf{nil}]^{\mathsf{s}}_{k}$ which respects the requirements of $\mathscr{R}$ such that $M \mid O \cong N \mid O$ and both systems $M \mid O \mid O'$ and $N \mid O \mid O'$ are well-formed. As $\cong$ is contextual and structural congruence is a monoid with respect to parallel composition, it follows that $(M \mid O') \mid O \equiv (M \mid O) \mid O' \cong (N \mid O) \mid O' \equiv (N \mid O') \mid O$. As $\equiv \subset \cong$ and $\cong$ is trivially transitive, this is enough to derive that $(M \mid O' \,,\, N \mid O') \in \mathscr{R}$.
- Let $(M,N) \in \mathscr{R}$. Let c be an arbitrary channel name. Let $O = n[\mathscr{I} \bowtie a!v.\mathsf{nil}]^{\mathsf{s}}_{k}$ which respects the requirements of $\mathscr{R}$. As $\cong$ is contextual if follows that $(\nu c)(M \mid O) \cong (\nu c)(N \mid O)$. Since O does not contain channels it holds that $((\nu c)M) \mid O \equiv (\nu c)(M \mid O) \cong (\nu c)(N \mid O) \equiv ((\nu c)N) \mid O$. As $\equiv \subset \cong$ and $\cong$ is trivially transitive, this is enough to derive that $((\nu c)M, (\nu c)N) \in \mathscr{R}$.
- Let $(M,N) \in \mathscr{R}$. Let $O = n[\mathscr{I} \bowtie a!v.\mathsf{nil}]^{\mathsf{s}}_{k}$ which respects the requirements of $\mathscr{R}$. Since O does not contain sensors, by Def. 5 we have: $M[s@h \mapsto v] \mid O = (M \mid O)[s@h \mapsto v] \cong (N \mid O)[s@h \mapsto v] = N[s@h \mapsto v] \mid O$. This is enough to derive that $(M[s@h \mapsto v], N[s@h \mapsto v]) \in \mathscr{R}$.

□

Proof of Theorem 6

Proof. For each law we exhibit the proper bisimulation. It is easy to see that for the first four laws the left-hand-side system evolves into the right-hand-side by performing a τ-actions. So, in order to prove these laws it is enough to show that the two terms under considerations are bisimilar. Let us proceed case by case.

1. Let use define the relation

$$\mathscr{R} = \big\{ \big(n[\mathscr{I} \bowtie a!v.P \mid R]^{\mu}_{h}, n[\mathscr{I} \bowtie P \mid R]^{\mu}_{h} \big) \mid \mathscr{I}(a) = v \text{ and } a \text{ does not occur in } R \big\} \cup Id$$

where Id is the identity relation. It suffices to prove the symmetric closure of $\mathscr{R}$ is a bisimulation.

2. Let us define the relation $\mathscr{R} = \big\{ \big(n[\mathscr{I} \bowtie @(x).P \mid R]^{\mu}_{h}, n[\mathscr{I} \bowtie P\{^{h}/_{x}\} \mid R]^{\mu}_{h} \big) \big\} \cup Id$, where Id is the identity relation. We show that the symmetric closure of $\mathscr{R}$ is a bisimulation. The proof is similar to that of Law 1 where $n[\mathscr{I} \bowtie @(x).P \mid R]^{\mu}_{h} \xrightarrow{\tau} n[\mathscr{I} \bowtie P\{^{h}/_{x}\} \mid R]^{\mu}_{h}$.

3. Let us define the relation $\mathscr{R} = \big\{ \big(n[\mathscr{I} \bowtie \lfloor \overline{c}\langle v \rangle.P \rfloor S \mid \lfloor c(x).Q \rfloor T \mid R]^{\mu}_{h} \, , \, n[\mathscr{I} \bowtie P \mid Q\{^{v}\!/_{x}\} \mid R]^{\mu}_{h} \big) \big\} \cup Id$, such that c is not in R and $\mathrm{rng}(c) = -1$. It suffices to show that the symmetric closure of $\mathscr{R}$ is a bisimulation.
4. The proof of Law 4 is similar to that of Law 3.
5. Let us define the relation $\mathscr{R} = \{ \big(n[\mathscr{I} \bowtie P]^{\mu}_{h}, n[\mathscr{I} \bowtie \mathsf{nil}]^{\mu}_{h} \big) \}$, where P does not contains terms of the form $\lfloor \pi.P_1 \rfloor P_2$ or $a!v.P_1$, for any a. It suffices to prove that the symmetric closure of $\mathscr{R}$ is a bisimulation.
6. Let us consider the relation $\mathscr{R} = \big\{ \big(n[\mathscr{I} \bowtie \mathsf{nil}]^{\mu}_{h}, \mathbf{0} \big) \mid \mathscr{I}(a)$ is undefined for any actuator $a \big\}$. It suffices to prove that the symmetric closure of $\mathscr{R}$ is a bisimulation.
7. Let us define the relation $\mathscr{R} = \{ (n[\emptyset \bowtie P]^{\mathtt{m}}_{h}, m[\emptyset \bowtie P]^{\mathtt{s}}_{k}) \}$, such that P does not contain terms $@(x).Q$ and for any channel c in P either $\mathrm{rng}(c) = \infty$ or $\mathrm{rng}(c) = -1$. It suffices to prove that the symmetric closure of $\mathscr{R}$ is a bisimulation.

□

Proof of Lemma 3

Proof. Let use define the relation $\mathscr{R}$ as follows:

$$\big\{ \big((\nu\tilde{c})(n[\mathscr{I} \bowtie P_1 | R]^{\mu}_{h} \mid O_1), (\nu\tilde{d})(n[\mathscr{I} \bowtie P_2 | R]^{\mu}_{k} \mid O_2) \big) : (\nu\tilde{c})(n[\mathscr{I} \bowtie P_1]^{\mu}_{h} \mid O_1) \approx (\nu\tilde{d})(n[\mathscr{I} \bowtie P_2]^{\mu}_{k} \mid O_2) \big\}$$

where process R can only (i) read the sensors of $\mathscr{I}$; (ii) transmit along some fresh Internet channel; (iii) let time passes. We prove that the symmetric closure of the relation $\mathscr{R}$ is a bisimulation. Let $(M,N) \in \mathscr{R}$, we proceed by case analysis on why $M \xrightarrow{\alpha} M'$.

- Let $M = (\nu\tilde{c})(n[\mathscr{I} \bowtie P_1 \mid R]^{\mu}_{h} \mid O_1) \xrightarrow{\alpha} (\nu\tilde{c})(n[\mathscr{I}' \bowtie P_1' \mid R]^{\mu}_{h'} \mid O_1') = M'$, with $\alpha \neq \sigma$, be a transitions which does not involve (and affect) R at all. This means that $(\nu\tilde{c})(n[\mathscr{I} \bowtie P_1]^{\mu}_{h} \mid O_1) \xrightarrow{\alpha} (\nu\tilde{c})(n[\mathscr{I}' \bowtie P_1']^{\mu}_{h'} \mid O_1')$. By hypothesis there are $\mathscr{I}''$, P_2', O_2' and k' such that $(\nu\tilde{c})(n[\mathscr{I} \bowtie P_2]^{\mu}_{k} \mid O_2) \xRightarrow{\alpha} (\nu\tilde{c})(n[\mathscr{I}'' \bowtie P_2']^{\mu}_{k'} \mid O_2')$ and $(\nu\tilde{c})(n[\mathscr{I}' \bowtie P_1']^{\mu}_{h'} \mid O_1') \approx (\nu\tilde{d})(n[\mathscr{I}'' \bowtie P_2']^{\mu}_{k'} \mid O_2')$. By Theorem 3 and Proposition 6 it follows that $\mathscr{I}' = \mathscr{I}''$. Furthermore as $\alpha \neq \sigma$ we have $h = h'$ and $k = k'$. Thus, $N = (\nu\tilde{c})(n[\mathscr{I} \bowtie P_2 \mid R]^{\mu}_{k} \mid O_2) \xRightarrow{\hat{\alpha}} (\nu\tilde{c})(n[\mathscr{I}' \bowtie P_2' \mid R]^{\mu}_{k'} \mid O_2') = N'$, with $(M',N') \in \mathscr{R}$.
- Let $M = (\nu\tilde{c})(n[\mathscr{I} \bowtie P_1 \mid R]^{\mu}_{h} \mid O_1) \xrightarrow{\sigma} (\nu\tilde{c})(n[\mathscr{I} \bowtie P_1' \mid R']^{\mu}_{h'} \mid O_1') = M'$. We know that timed actions do not change the physical interface $\mathscr{I}$. This implies that: (i) $R \xrightarrow{\sigma} R'$; (ii) $(\nu\tilde{c})(n[\mathscr{I} \bowtie P_1 \mid R]^{\mu}_{h} \mid O_1) \stackrel{\tau}{\not\longrightarrow}$; (iii) $(\nu\tilde{c})(n[\mathscr{I} \bowtie P_1]^{\mu}_{h} \mid O_1) \xrightarrow{\sigma} (\nu\tilde{c})(n[\mathscr{I} \bowtie P_1']^{\mu}_{h'} \mid O_1')$. In particular, the second item means that R does not have any interaction with the network. It even does not read some sensor of $\mathscr{I}$. By hypothesis we have that $(\nu\tilde{c})(n[\mathscr{I} \bowtie P_2]^{\mu}_{k} \mid O_2) \Rightarrow \xrightarrow{\sigma} \Rightarrow (\nu\tilde{c})(n[\mathscr{I}' \bowtie P_2']^{\mu}_{k'} \mid O_2')$ with $(\nu\tilde{c})(n[\mathscr{I} \bowtie P_1']^{\mu}_{h'} \mid O_1') \approx (\nu\tilde{d})(n[\mathscr{I}' \bowtie P_2']^{\mu}_{k'} \mid O_2')$. By Theorem 3 and Proposition 6 we know that it must be $\mathscr{I} = \mathscr{I}'$. As R cannot have any interaction with the rest of the network, apart from time synchronisation, it follows that $N = (\nu\tilde{c})(n[\mathscr{I} \bowtie P_2 \mid R]^{\mu}_{k} \mid O_2) \Rightarrow \xrightarrow{\sigma} \Rightarrow (\nu\tilde{c})(n[\mathscr{I} \bowtie P_2' \mid R']^{\mu}_{k'} \mid O_2') = N'$, with $(M',N') \in \mathscr{R}$.
- Let $M = (\nu\tilde{c})(n[\mathscr{I} \bowtie P_1 \mid R]^{\mu}_{h} \mid O_1) \xrightarrow{\alpha} (\nu\tilde{c})(n[\mathscr{I} \bowtie P_1 \mid R']^{\mu}_{h} \mid O_1') = M'$, with $\alpha \neq \sigma$, be a transitions which is due to R. This can be a sensor reading or a transmission along some channel b, with $\mathrm{rng}(b) = \infty$. In that case, it is easy to see that, as $\mathrm{rng}(b) = \infty$, then $N = (\nu\tilde{c})(n[\mathscr{I} \bowtie P_2 \mid R]^{\mu}_{k} \mid O_2) \xrightarrow{\alpha} (\nu\tilde{c})(n[\mathscr{I} \bowtie P_2 \mid R']^{\mu}_{k} \mid O_2) = N'$, with $(M',N') \in \mathscr{R}$.

□

Proof of Proposition 10

Proof. Let us rename the processes to save space: $L \overset{\text{def}}{=} \mathit{LightCtrl}$, $\overline{L} \overset{\text{def}}{=} \overline{\mathit{LightCtrl}}$, $L_1 \overset{\text{def}}{=} \mathit{LightMng}_1$, $L_2 \overset{\text{def}}{=} \mathit{LightMng}_2$, and $\overline{C} \overset{\text{def}}{=} \overline{\mathit{CLightMng}}$. Let us define the relation

$$\mathscr{R} \overset{\text{def}}{=} \bigcup_{i=1}^{17} \Big((\nu \tilde{c}) M_i \,,\, (\nu \tilde{c})(\nu g) N_i \Big)$$

where the pairs (M_i, N_i), for $1 \le i \le 17$, are listed below:

- $M_1 = n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{k} \mid n_1[\mathscr{I}_1 \bowtie L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4}$
  $N_1 = n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{k} \mid n_1[\mathscr{I}_1 \bowtie L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4} \mid n_C[\emptyset \bowtie \sigma.\overline{C}]^{\mathtt{s}}_{loc3}$
  with $k \notin \{loc1, loc2, loc3, loc4\}$, $\mathscr{I}_1(\mathit{light}_1) = \mathsf{off}$ and $\mathscr{I}_2(\mathit{light}_2) = \mathsf{off}$
- $M_2 = n_P[\mathscr{I}_P \bowtie \sigma.L]^{\mathtt{m}}_{loc1} \mid n_1[\mathscr{I}_1 \bowtie \mathit{light}_1!\mathsf{on}.\sigma.L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4}$
  $N_2 = n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{loc1} \mid n_1[\mathscr{I}_1 \bowtie \mathit{light}_1!\mathsf{on}.\sigma.L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4} \mid n_C[\emptyset \bowtie \sigma.\overline{C}]^{\mathtt{s}}_{loc3}$
- $M_3 = n_P[\mathscr{I}_P \bowtie \sigma.L]^{\mathtt{m}}_{loc1} \mid n_1[\mathscr{I}'_1 \bowtie \sigma.L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4}$
  $N_3 = n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{loc1} \mid n_1[\mathscr{I}'_1 \bowtie \sigma.L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4} \mid n_C[\emptyset \bowtie \sigma.\overline{C}]^{\mathtt{s}}_{loc3}$
  with $\mathscr{I}'_1(\mathit{light}_1) = \mathsf{on}$.
- $M_4 = n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{k} \mid n_1[\mathscr{I}'_1 \bowtie L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4}$
  $N_4 = n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{k} \mid n_1[\mathscr{I}'_1 \bowtie L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4} \mid n_C[\emptyset \bowtie \sigma.\overline{C}]^{\mathtt{s}}_{loc3}$
  with $k \notin \{loc1, loc2, loc3, loc4\}$
- $M_5 = n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{k} \mid n_1[\mathscr{I}'_1 \bowtie \mathit{light}_1!\mathsf{off}.L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4}$
  $N_5 = n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{k} \mid n_1[\mathscr{I}'_1 \bowtie \mathit{light}_1!\mathsf{off}.L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4} \mid n_C[\emptyset \bowtie \sigma.\overline{C}]^{\mathtt{s}}_{loc3}$
  with $k \notin \{loc1, loc2, loc3, loc4\}$
- $M_6 = n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{loc1} \mid n_1[\mathscr{I}'_1 \bowtie \mathit{light}_1!\mathsf{off}.L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4}$
  $N_6 = n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{loc1} \mid n_1[\mathscr{I}'_1 \bowtie \mathit{light}_1!\mathsf{off}.L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4} \mid n_C[\emptyset \bowtie \lfloor \overline{c_1}\langle \mathsf{on} \rangle.\sigma.\overline{C} \rfloor CLM]^{\mathtt{s}}_{loc3}$
- $M_7 = n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{loc2} \mid n_1[\mathscr{I}'_1 \bowtie L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4}$
  $N_7 = n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{loc2} \mid n_1[\mathscr{I}'_1 \bowtie L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4} \mid n_C[\emptyset \bowtie \sigma.\overline{C}]^{\mathtt{s}}_{loc3}$
- $M_8 = n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{loc3} \mid n_1[\mathscr{I}'_1 \bowtie \mathit{light}_1!\mathsf{off}.L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4}$
  $N_8 = n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{loc3} \mid n_1[\mathscr{I}'_1 \bowtie \mathit{light}_1!\mathsf{off}.L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4} \mid n_C[\emptyset \bowtie \sigma.\overline{C}]^{\mathtt{s}}_{loc3}$
- $M_9 = n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{loc2} \mid n_1[\mathscr{I}'_1 \bowtie \mathit{light}_1!\mathsf{off}.L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4}$
  $N_9 = n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{loc2} \mid n_1[\mathscr{I}'_1 \bowtie \mathit{light}_1!\mathsf{off}.L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4} \mid n_C[\emptyset \bowtie \sigma.\overline{C}]^{\mathtt{s}}_{loc3}$
- $M_{10} = n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{loc3} \mid n_1[\mathscr{I}_1 \bowtie L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4}$
  $N_{10} = n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{loc3} \mid n_1[\mathscr{I}_1 \bowtie L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4} \mid n_C[\emptyset \bowtie \sigma.\overline{C}]^{\mathtt{s}}_{loc3}$
- $M_{11} = n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{loc2} \mid n_1[\mathscr{I}_1 \bowtie L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4}$
  $N_{11} = n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{loc2} \mid n_1[\mathscr{I}_1 \bowtie L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4} \mid n_C[\emptyset \bowtie \sigma.\overline{C}]^{\mathtt{s}}_{loc3}$
- $M_{12} = n_P[\mathscr{I}_P \bowtie \sigma.L]^{\mathtt{m}}_{loc4} \mid n_1[\mathscr{I}_1 \bowtie L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie \mathit{light}_2!\mathsf{on}.\sigma.L_2]^{\mathtt{s}}_{loc4}$
  $N_{12} = n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{loc4} \mid n_1[\mathscr{I}_1 \bowtie L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie \mathit{light}_2!\mathsf{on}.\sigma.L_2]^{\mathtt{s}}_{loc4} \mid n_C[\emptyset \bowtie \sigma.\overline{C}]^{\mathtt{s}}_{loc3}$
- $M_{13} = n_P[\mathscr{I}_P \bowtie \sigma.L]^{\mathtt{m}}_{loc4} \mid n_1[\mathscr{I}_1 \bowtie L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}'_2 \bowtie \sigma.L_2]^{\mathtt{s}}_{loc4}$
  $N_{13} = n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{loc4} \mid n_1[\mathscr{I}_1 \bowtie L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}'_2 \bowtie \sigma.L_2]^{\mathtt{s}}_{loc4} \mid n_C[\emptyset \bowtie \sigma.\overline{C}]^{\mathtt{s}}_{loc3}$
  where $\mathscr{I}'_2(\mathit{light}_2) = \mathsf{on}$
- $M_{14} = n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{loc3} \mid n_1[\mathscr{I}_1 \bowtie L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}'_2 \bowtie L_2]^{\mathtt{s}}_{loc4}$
  $N_{14} = n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{loc3} \mid n_1[\mathscr{I}_1 \bowtie L_1]^{\mathtt{s}}_{loc1} \mid n_2[\mathscr{I}'_2 \bowtie L_2]^{\mathtt{s}}_{loc4} \mid n_C[\emptyset \bowtie \sigma.\overline{C}]^{\mathtt{s}}_{loc3}$

- $M_{15} = n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{loc4} \mid n_1[\mathscr{I}_1 \bowtie L_1]^{\mathsf{s}}_{loc1} \mid n_2[\mathscr{I}_2' \bowtie light_2!\mathsf{off}.L_2]^{\mathsf{s}}_{loc4}$
  $N_{15} = n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{loc4} \mid n_1[\mathscr{I}_1 \bowtie L_1]^{\mathsf{s}}_{loc1} \mid n_2[\mathscr{I}_2' \bowtie light_2!\mathsf{off}.L_2]^{\mathsf{s}}_{loc4} \mid n_C[\emptyset \bowtie \lfloor \overline{c_2}\langle \mathsf{on} \rangle.\sigma.\overline{C} \rfloor \overline{C}]^{\mathsf{s}}_{loc3}$
- $M_{16} = n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{loc2} \mid n_1[\mathscr{I}_1 \bowtie L_1]^{\mathsf{s}}_{loc1} \mid n_2[\mathscr{I}_2' \bowtie light_2!\mathsf{off}.L_2]^{\mathsf{s}}_{loc4}$
  $N_{16} = n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{loc2} \mid n_1[\mathscr{I}_1 \bowtie L_1]^{\mathsf{s}}_{loc1} \mid n_2[\mathscr{I}_2' \bowtie light_2!\mathsf{off}.L_2]^{\mathsf{s}}_{loc4} \mid n_C[\emptyset \bowtie \sigma.\overline{C}]^{\mathsf{s}}_{loc3}$
- $M_{17} = n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{loc3} \mid n_1[\mathscr{I}_1 \bowtie L_1]^{\mathsf{s}}_{loc1} \mid n_2[\mathscr{I}_2' \bowtie light_2!\mathsf{off}.L_2]^{\mathsf{s}}_{loc4}$
  $N_{17} = n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{loc3} \mid n_1[\mathscr{I}_1 \bowtie L_1]^{\mathsf{s}}_{loc1} \mid n_2[\mathscr{I}_2' \bowtie light_2!\mathsf{off}.L_2]^{\mathsf{s}}_{loc4} \mid n_C[\emptyset \bowtie \sigma.\overline{C}]^{\mathsf{s}}_{loc3}$.

For each pair $\big((\nu\tilde{c})M_i\,,\,(\nu\tilde{c},g)N_i\big) \in \mathscr{R}$ we proceed by case analysis on why $(\nu\tilde{c})M_i \xrightarrow{\alpha} \hat{M}$. Then, we do the same for $(\nu\tilde{c},g)N_i \xrightarrow{\alpha} \hat{N}$. Before starting the case analysis we notice that in all pairs of $\mathscr{R}$ the physical interfaces of the corresponding nodes are the same. For that reason we can safely omit the extensional actions of the form $a@h!v$. Moreover, our processes never read sensors (we removed from the initial system both the process *BoilerCtrl* and the network *BM*). Thus, we can safely omit transitions labelled with actions of the form $s@h?v$ as well.

– Let us consider the pair $\big((\nu\tilde{c})M_1\,,\,(\nu\tilde{c})(\nu g)N_1\big)$. We proceed by case analysis on why $(\nu\tilde{c})M_1 \xrightarrow{\alpha} \hat{M}$.

- Let $(\nu\tilde{c})M_1 \xrightarrow{\alpha} \hat{M}$, for $\alpha \neq \sigma$. This case is not admissible as the phone is too far to interact with some local light manager.
- Let $(\nu\tilde{c})M_1 \xrightarrow{\sigma} (\nu\tilde{c})M_1'$, with

  $$M_1' = n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{k} \mid n_1[\mathscr{I}_1 \bowtie light_I!\mathsf{off}.L_1]^{\mathsf{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie light_2!\mathsf{off}.L_2]^{\mathsf{s}}_{loc4}$$

  and $k \notin \{loc1, loc2, loc3, loc4\}$. This means that the phone didn't get inside the smarthome. By the sake of simplicity we will call k all locations outside the smarthome. By two applications of Law 1 of Theorem 6 we have: $(\nu\tilde{c})M_1' \gtrsim (\nu\tilde{c})\big(n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{k} \mid n_1[\mathscr{I}_1 \bowtie L_1]^{\mathsf{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathsf{s}}_{loc4}\big) = (\nu\tilde{c})M_1$. Then, $(\nu\tilde{c},g)N_1 \xrightarrow{\sigma}\Rightarrow (\nu\tilde{c},g)N_1$, and $\big((\nu\tilde{c})M_1\,,\,(\nu\tilde{c},g)N_1\big) \in \mathscr{R}$.
- Let $(\nu\tilde{c})M_1 \xrightarrow{\sigma} (\nu\tilde{c})M_1'$, with

  $$M_1' = n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{loc1} \mid n_1[\mathscr{I}_1 \bowtie light_1!\mathsf{off}.L_1]^{\mathsf{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie light_2!\mathsf{off}.L_2]^{\mathsf{s}}_{loc4} \ .$$

  In this case the smartphone just entered the smarthome from its entrance, located at $loc1$. By two applications of Law 1 and one application of Law 4 of Theorem 6 we have:

  $$(\nu\tilde{c})M_1' \gtrsim (\nu\tilde{c})\big(n_P[\mathscr{I}_P \bowtie \sigma.L]^{\mathtt{m}}_{loc1} \mid n_1[\mathscr{I}_1 \bowtie light_1!\mathsf{on}.\sigma.L_1]^{\mathsf{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathsf{s}}_{loc4}\big) = (\nu\tilde{c})M_2 \ .$$

  Then, there is N_2 such that $(\nu\tilde{c},g)N_1 \xrightarrow{\sigma}\Rightarrow (\nu\tilde{c},g)N_2$ with

  $$(\nu\tilde{c},g)N_2 = (\nu\tilde{c},g)\big(n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{loc1} \mid n_1[\mathscr{I}_1 \bowtie light_1!\mathsf{on}.\sigma.L_1]^{\mathsf{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie L_2]^{\mathsf{s}}_{loc4} \mid n_C[\emptyset \bowtie \sigma.\overline{C}]^{\mathsf{s}}_{loc3}\big)$$

  and $\big((\nu\tilde{c})M_2\,,\,(\nu\tilde{c},g)N_2\big) \in \mathscr{R}$.

Now, we proceed by case analysis on why $(\nu\tilde{c},g)N_1 \xrightarrow{\alpha} \hat{N}$.

- Let $(\nu\tilde{c},g)N_1 \xrightarrow{\alpha} \hat{N}$, with $\alpha \neq \sigma$. This case is not admissible.
- Let $(\nu\tilde{c},g)N_1 \xrightarrow{\sigma} (\nu\tilde{c},g)N_1'$, where the phone didn't enter the house, as its location is different from $loc1$. This case is similar to the previous one.
- $(\nu\tilde{c},g)N_1 \xrightarrow{\sigma} (\nu\tilde{c},g)N_1'$, with

  $$N_1' = n_P[\mathscr{I}_P \bowtie \overline{L}]^{\mathtt{m}}_{loc1} \mid n_1[\mathscr{I}_1 \bowtie light_1!\mathsf{off}.L_1]^{\mathsf{s}}_{loc1} \mid n_2[\mathscr{I}_2 \bowtie light_2!\mathsf{off}.L_2]^{\mathsf{s}}_{loc4} \mid n_C[\emptyset \bowtie \overline{C}]^{\mathsf{s}}_{loc3} \ .$$

Because the phone just moved to location $loc1$. By two applications of Law 1, one applications of Law 2, and two applications of Law 4 of Theorem 6 we have:

$$\begin{array}{rcl}(\nu\tilde{c},g)N_1' & \gtrsim & (\nu\tilde{c},g)\big(n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{loc1} \,|\, n_1[\mathscr{I}_1 \bowtie light_1!\mathsf{on}.\sigma.L_1]^{\mathtt{s}}_{loc1} \,|\, n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4} \,|\, n_C[\emptyset \bowtie \sigma.\overline{C}]^{\mathtt{s}}_{loc3}\big) \\ & = & (\nu\tilde{c},g)N_2 \ .\end{array}$$

Then, there is M_2 such that $(\nu\tilde{c})M_1 \xrightarrow{\sigma}\Rightarrow (\nu\tilde{c})M_2$, with

$$M_2 \ = \ n_P[\mathscr{I}_P \bowtie \sigma.L]^{\mathtt{m}}_{loc1} \ \big| \ n_1[\mathscr{I}_1 \bowtie light_1!\mathsf{on}.\sigma.L_1]^{\mathtt{s}}_{loc1} \ \big| \ n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4}$$

and $\big((\nu\tilde{c})M_2\,,\,(\nu\tilde{c},g)N_2\big) \in \mathscr{R}$.

– Let us consider the pair $\big((\nu\tilde{c})M_2\,,\,(\nu\tilde{c})(\nu g)N_2\big)$. The only possible transition in both networks is a strong transition $\xrightarrow{light_l}$ which leads to the pair $\big((\nu\tilde{c})M_3\,,\,(\nu\tilde{c})(\nu g)N_3\big) \in \mathscr{R}$.

– Let us consider the pair $\big((\nu\tilde{c})M_3\,,\,(\nu\tilde{c})(\nu g)N_3\big)$. We proceed by case analysis on why $(\nu\tilde{c})M_3 \xrightarrow{\alpha} \hat{M}$.

- Let $(\nu\tilde{c})M_3 \xrightarrow{\alpha} \hat{M}$, for $\alpha \neq \sigma$. This case is not admissible.
- Let $(\nu\tilde{c})M_3 \xrightarrow{\sigma} (\nu\tilde{c})M_3'$, where $M_3' = n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{loc1} \,\big|\, n_1[\mathscr{I}_1' \bowtie L_1]^{\mathtt{s}}_{loc1} \,\big|\, n_2[\mathscr{I}_2 \bowtie light_2!\mathsf{off}.L_2]^{\mathtt{s}}_{loc4}$ because the phone remained at location $loc1$. By two applications of Law 1 and one application of Law 4 of Theorem 6 we get:

  $$(\nu\tilde{c})M_3' \ \gtrsim \ (\nu\tilde{c})\big(n_P[\mathscr{I}_P \bowtie \sigma.L]^{\mathtt{m}}_{loc1} \,|\, n_1[\mathscr{I}_1' \bowtie \sigma.L_1]^{\mathtt{s}}_{loc1} \,|\, n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4}\big) \ = \ (\nu\tilde{c})M_3 \ .$$

  Then, $(\nu\tilde{c},g)N_3 \xrightarrow{\sigma}\Rightarrow (\nu\tilde{c},g)N_3$, and obviously $\big((\nu\tilde{c})M_3\,,\,(\nu\tilde{c},g)N_3\big) \in \mathscr{R}$.
- Let $(\nu\tilde{c})M_3 \xrightarrow{\sigma} (\nu\tilde{c})M_3'$, where $M_3' = n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{k} \,\big|\, n_1[\mathscr{I}_1' \bowtie L_1]^{\mathtt{s}}_{loc1} \,\big|\, n_2[\mathscr{I}_2 \bowtie light_2!\mathsf{off}.L_2]^{\mathtt{s}}_{loc4}$, with $k \notin \{loc1, loc2, loc3, loc4\}$, i.e. the phone moved out of the house. By applying Law 1 of Theorem 6 we get $(\nu\tilde{c})M_3' \ \gtrsim \ (\nu\tilde{c})n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{k} \,\big|\, n_1[\mathscr{I}_1' \bowtie L_1]^{\mathtt{s}}_{loc1} \,\big|\, n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4} \ = \ (\nu\tilde{c})M_4$. Then, there is N_4 such that $(\nu\tilde{c},g)N_3 \xrightarrow{\sigma}\Rightarrow (\nu\tilde{c},g)N_4$ with:

  $$N_4 = n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{k} \ \big| \ n_1[\mathscr{I}_1' \bowtie L_1]^{\mathtt{s}}_{loc1} \ \big| \ n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4} \ \big| \ n_C[\emptyset \bowtie \sigma.\overline{C}]^{\mathtt{s}}_{loc3}$$

  and $\big((\nu\tilde{c})M_4\,,\,(\nu\tilde{c},g)N_4\big) \in \mathscr{R}$.
- Let $(\nu\tilde{c})M_3 \xrightarrow{\sigma} (\nu\tilde{c})M_3'$, where $M_3' = n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{loc2} \,\big|\, n_1[\mathscr{I}_1' \bowtie L_1]^{\mathtt{s}}_{loc1} \,\big|\, n_2[\mathscr{I}_2 \bowtie light_2!\mathsf{off}.L_2]^{\mathtt{s}}_{loc4}$, because the phone moved from $loc1$ to $loc2$. In this case, by applying Law 1 of Theorem 6 we have:

  $$(\nu\tilde{c})M_3' \ \gtrsim \ (\nu\tilde{c})\big(n_P[\mathscr{I}_P \bowtie L]^{\mathtt{m}}_{loc2} \,|\, n_1[\mathscr{I}_1' \bowtie L_1]^{\mathtt{s}}_{loc1} \,|\, n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4}\big) \ = \ (\nu\tilde{c})M_7 \ .$$

  Then, we have that $(\nu\tilde{c},g)N_3 \xrightarrow{\sigma}\Rightarrow (\nu\tilde{c},g)N_7$, where

  $$N_7 \ = \ n_P[\mathscr{I}_P \bowtie \sigma.\overline{L}]^{\mathtt{m}}_{loc2} \,\big|\, n_1[\mathscr{I}_1' \bowtie L_1]^{\mathtt{s}}_{loc1} \,\big|\, n_2[\mathscr{I}_2 \bowtie L_2]^{\mathtt{s}}_{loc4} \,\big|\, n_C[\emptyset \bowtie \sigma.\overline{C}]^{\mathtt{s}}_{loc3}$$

  and $\big((\nu\tilde{c})M_7\,,\,(\nu\tilde{c},g)N_7\big) \in \mathscr{R}$.

The case analysis when $(\nu\tilde{c},g)N_3 \xrightarrow{\alpha} \hat{N}$ is similar.

The remaining cases, dealing with the pairs $\big((\nu\tilde{c})M_i\,,\,(\nu\tilde{c})(\nu g)N_i\big)$, for $4 \leq i \leq 17$, work in a similar manner. □