A Timed Calculus for Wireless Systems *†

Massimo Merro and Eleonora Sibilio

Dipartimento di Informatica, Università degli Studi di Verona, Italy

Abstract

We propose a *timed process calculus* for *wireless systems* exposed to *communication collisions*. The operational semantics of our calculus is given in terms of a *labelled transition system*. The calculus enjoys a number of desirable time properties such as (i) *time determinism*: the passage of time is deterministic; (ii) *patience*: devices will wait indefinitely until they can communicate; (iii) *maximal progress*: data transmissions cannot be delayed, they must occur as soon as a possibility for communication arises. As a case study we use our calculus to model the *Carrier Sense Multiple Access* (CSMA) scheme.

The main behavioural equality of our calculus is a timed variant of *barbed congruence*, a standard branching-time and contextually-defined program equivalence. As an efficient proof method for timed barbed congruence we define a labelled bisimilarity. We then apply our bisimulation proof-technique to prove a number of algebraic properties.

1 Introduction

Wireless technology spans from user applications such as personal area networks, ambient intelligence, and wireless local area networks, to real-time applications, such as cellular, and ad hoc networks. The IEEE 802.11 standard [19] contains a series of specifications for wireless LAN technologies. The basic building block of an 802.11 network is the *basic service set* (BBS), which is a set of stations that have successfully synchronised and that use radio transceivers to broadcast messages. In *independent* BBS (IBBS), stations communicate with each other

*This work was partially supported by the PRIN 2007 project "SOFT".

†An extended abstract will appear in the proceedings of the *3rd International Conference on Fundamentals of Software Engineering* (FSEN'09) Kish Island, Iran.

without using any *distribution system*. IBBS networks are sometimes referred to as *ad hoc networks*. In this paper, we propose a formal model for IBBS networks paying particular attention to *communication interferences*. Communication interferences represent one of the main concern when evaluating the performances of a network in terms of *network throughput*, i.e. the average rate of successful message delivery over a communication channel.

In concurrent systems, an interference occurs when the activity of a component is damaged or corrupted because of the activities of another component. In Ethernet-like networks communication channels are full-duplex; that is, a node can transmit and receive at the same time. As a consequence, *collisions* caused by two simultaneous transmissions are immediately detected and repaired by retransmitting the message after a randomly-chosen period of time. This is not possible in wireless networks where radio signals span over a limited area, called *transmission cell*, and channels are *half-duplex*: on a given channel, a device can either transmit or receive, but cannot do both at the same time. As a consequence, in wireless systems communication collisions can only be detected at destination by receivers exposed to different transmissions.

In the last twenty-five years, process calculi [25, 6, 26, 8, 18] have been intensively used to study the semantics of concurrent/distributed systems, and to develop verification techniques for such systems. In the literature, there exist a number of process calculi modelling wireless systems [24, 30, 37, 23, 14, 15, 12, 13]. All these calculi rely on the presence of some MAC-level protocol to remove interferences. However, in wireless systems *collisions cannot be avoided* although there are protocols to reduce their occurrences (see, for instance, the IEEE 802.11 CSMA/CA protocol [19] for unicast communications). We believe that communication collisions represent a serious concern that should be taken into account in a timed model for wireless systems.

Many protocols for wireless networks rely on a *common notion of time* among the devices, provided by some *clock synchronisation protocol*. Most clock synchronisation protocols for ad hoc networks [28, 11, 36, 38, 22, 42] follow the "clock correction" approach correcting the local clock of each node to run in par with a global time scale. [1] This approach heavily rely on *network connectivity*. In a connected network all nodes are in touch with each other, although not always directly. Wireless networks are usually assumed to be connected; disconnected devices can be considered as not being part of the network as, in general, they need to re-authenticate to rejoin the network.

In this paper, we propose a *timed calculus* for wireless networks, called TCWS, in which all wireless devices are assumed to be *synchronised* (using some clock-

[1] An excellent survey of existing clock synchronisation protocols for sensor networks (and more generally for ad-hoc networks) can be found in [39].

correction synchronisation protocol). Thus, TCWS is a process calculus with *absolute timing*, where all timing refers to an absolute clock. Time proceeds in *discrete* steps represented by occurrences of a simple action σ, in the style of Hennessy and Regan's TPL [17], to denote idling until the next clock cycle. The calculus is value-passing, and message transmission requires a positive amount of time. We follow a *two-phase* approach [31] separating the execution of actions from the passage of time. As in Hennessy and Regan's TPL [17], and Prasad's timed CBS [33], our TCWS enjoys three basic time properties:

- *time determinism*: the passage of time is deterministic, i.e. a network can reach at most one new state by performing the action σ;
- *patience*: nodes will wait indefinitely until they can communicate;
- *maximal progress*: data transmissions cannot be delayed, they must occur as soon as a possibility for communication arises.

The operational semantics of our calculus is given in terms of a *labelled transition system* (LTS) in the SOS style of Plotkin. As usual for ad hoc networks, the communication mechanism is *broadcast*. We provide a notion of network well-formedness to take into account node-uniqueness, network connectivity, transmission exposure, and transmission consistency. We then prove that our labelled transition semantics preserves network well-formedness.

As a case study we use our calculus to model the *Carrier Sense Multiple Access* (CSMA) scheme [19]. According to the CSMA scheme, stations transmit only when the channel is sensed free. As we will show, this protocol allows to prevent certain form of collisions, although it suffers of two well-known problems: the *hidden terminal problem* and the *exposed terminal problem*.

A central concern in process calculi is to establish when two terms have the same *observable behaviour*, that is, they are indistinguishable in any context. *Behavioural equivalences* are fundamental for justifying program transformations. Our program equivalence is a timed variant of (weak) *reduction barbed congruence*, a branching-time contextually-defined program equivalence. Barbed equivalences [27] are simple and intuitive but difficult to use due to the quantification on all contexts. Simpler proof techniques are based on *labelled bisimilarities* [25], which are co-inductive relations that characterise the behaviour of processes using a *labelled transition system*. We define a *labelled bisimilarity* which is a proof method for timed reduction barbed congruence. We then apply our bisimulation proof-technique to prove a number of algebraic properties.

We end this introduction with an outline of the paper. In Section 2, we provide both syntax and operational semantics of our calculus. In the same section we

Table 1 The Syntax

Values			
u	$::=$	x	variable
	$\mid$	v	closed value
Networks:			
M, N	$::=$	$\mathbf{0}$	empty network
	$\mid$	$M_1 \mid M_2$	parallel composition
	$\mid$	$n[W]_t^\nu$	node
Processes:			
W	$::=$	P	inactive process
	$\mid$	A	active process
P, Q	$::=$	nil	termination
	$\mid$	$!\langle u\rangle.P$	broadcast
	$\mid$	$?(x).P$	receiver
	$\mid$	$\sigma.P$	delay
	$\mid$	$\lfloor ?(x).P \rfloor Q$	receiver with timeout
	$\mid$	$[u_1 = u_2]P, Q$	matching
	$\mid$	$H\langle \tilde{u}\rangle$	recursion
A	$::=$	$\langle v\rangle^t.P$	active sender
	$\mid$	$(x)_v.P$	active receiver

propose a notion of network well-formedness to rule out inconsistent networks. In Section 3, we prove that TCWS enjoys the following time properties: time determinism, maximal progress and patience. We also prove that network well-formedness is preserved at run time. In Section 4, we use our calculus to study the CSMA protocol. In Section 5, we equip TCWS with a notion of observational equivalence along the lines of Milner and Sangiorgi's barbed congruence. In Section 6, we propose a labelled bisimilarity as a proof method for our observations equivalence. More precisely, we prove that our bisimilarity is a congruence and that it implies our observational equivalence. We then use our bisimilarity to prove a number of algebraic properties. Finally, in Section 7 we present, in some detail, future and related works.

2 The Calculus

In Table 1, we define the syntax of TCWS in a two-level structure, a lower one for *processes* and a upper one for *networks*. We use letters $a, b, c, \ldots$ for logical names, x, y, z for *variables*, u for *values*, and v and w for *closed values*, i.e. values that do not contain free variables. Closed values actually denote messages that are transmitted as TCP/IP packets. Packets contain a number of auxiliary informations such as the network address of the transmitter. So, sometimes we write $m{:}v$ to mean a message v transmitted by node m. With an abuse of notation, structured messages of the form $m{:}v$ are ranged by the same letters v and w. We write $\tilde{u}$ to denote a tuple $u_1, \ldots, u_k$ of values.

Networks are collections of nodes (which represent devices) running in parallel and using a unique common channel to communicate with each other. We use the symbol $\mathbf{0}$ to denote an empty network, while $M_1 \mid M_2$ represents the parallel composition of two sub-networks M_1 and M_2. Nodes cannot be created or destroyed. All nodes have the same transmission range. We write $n[W]_t^\nu$ for a node named n (the device network address) executing the sequential process W. The tag ν denotes the set of (the names of) the neighbours of n. Said in other words, ν contains all nodes in the transmission cell of n. In this manner, we model the network topology. Notice that the network topology could have been represented using some kind of restriction operator à la CCS over node names. We preferred our notation to keep at hand the neighbours of a node. The variable t is a semantic tag ranging over positive integers to represent *node exposure*. Thus, a node $n[W]_t^\nu$, with $t > 0$, is exposed to a transmission (or more transmissions) for the next t instants of time.

Processes are sequential and live within the nodes. For convenience, we distinguish between *non-active* and *active processes*. An active process is a process which is currently transmitting or receiving. An *active node* is a node with an active process inside. The symbol nil denotes the skip process. The sender process $!\langle v\rangle.P$ allows to broadcast the value v. Once the transmission starts the process evolves into the active sender process $\langle v\rangle^{\delta_v}.P$ which transmits the message v for the next δ_v time units, the time necessary to transmit v. In the construct $\langle v\rangle^t.P$ we require $t > 0$. The receiver process $?(x).P$ listens on the channel for incoming messages. Once the reception starts the process evolves into the active receiver process $(x)_w.P$ and starts receiving. Only when the channel becomes free the receiver calculates the CRC to check the integrity of the received packets. Upon successful reception the variable x of P is instantiated with the transmitted message w. The process $\sigma.P$ models sleeping for one time unit. The process $\lfloor ?(x).P \rfloor Q$ denotes a receiver with timeout. [2] Intuitively, this process either starts

[2] This operator comes from the process algebra ATP put forward in [31].

receiving a value in the current instant of time, evolving into an active receiver, or it idles for one time unit, and then continues as Q. Process $[v_1 = v_2]P, Q$ is the standard "if then else" construct: it behaves as P if $v_1 = v_2$, and as Q otherwise. In processes $\sigma.P, ?(x).P$, $\lfloor ?(x).P \rfloor Q$, and $!\langle v \rangle.P$ the occurrence of process P is said to be *guarded*. We write $H\langle \tilde{v} \rangle$ to denote a process defined via a definition $H(\tilde{x}) \stackrel{\text{def}}{=} P$, with $\mid \tilde{x} \mid = \mid \tilde{v} \mid$, where $\tilde{x}$ contains all variables that appear free in P. Defining equations provide *guarded recursion*, since P may contain only guarded occurrences of process identifiers, such as H itself. We use a number of notational conventions. $\prod_{i \in I} M_i$ means the parallel composition of all sub-networks M_i, for $i \in I$. We write $!\langle v \rangle$ for $!\langle v \rangle.\mathsf{nil}$, and $\langle v \rangle^\delta$ for $\langle v \rangle^\delta.\mathsf{nil}$. We recall that in the active sender process $\langle v \rangle^t.P$ it holds that $t > 0$. However, sometimes, for convenience, we write $\langle v \rangle^0.P$ assuming the following syntactic equality $\langle v \rangle^0.P = P$.

In the terms $?(x).P$, $\lfloor ?(x).P \rfloor Q$, and $(x)_v.P$ the variable x is bound in P. This gives rise to the standard notion of α-conversion. We identify processes and networks up to α-conversion. We assume there are no free variables in our networks. The absence of free variables in networks is trivially maintained as the network evolves. We write $\{^v/_x\}P$ for the substitution of the variable x with the value v in P. We define *structural congruence*, written $\equiv$, as the smallest congruence which is a commutative monoid with respect to the parallel operator.

Given a network M, $\mathsf{nds}(M)$ returns the names of the nodes which constitute the network M. For any network M, $\mathsf{actsnd}(M)$ and $\mathsf{actrcv}(M)$ return the set of active senders and active receivers of M, respectively. Thus, for instance, for $N = m[!\langle w \rangle]^\nu_t \mid n[\langle v \rangle^r.P]^{\nu'}_{t'}$ we have $\mathsf{nds}(N) = \{m, n\}$ and $\mathsf{actsnd}(N) = \{n\}$. Given a network M and an active sender $n \in \mathsf{actsnd}(M)$, the function $\mathsf{active}(n, M)$ says for how long the node will be transmitting. For instance, if N is the network defined as before, $\mathsf{active}(n, N) = r$. If n is not an active sender then $\mathsf{active}(n, N) = 0$. Finally, given a network M and a node $m \in \mathsf{nds}(M)$, the function $\mathsf{ngh}(m, M)$ returns the set of neighbours of m in M. Thus, for N defined as above $\mathsf{ngh}(m, N) = \nu$.

2.1 The Operational Semantics

We give the operational semantics of our calculus in terms of a Labelled Transition System (LTS). Table 2 contains a simple LTS for processes. Rules (SndP) and (RcvP) model the beginning of a transmission. In rule (SndP) a sender evolves into an active sender. For convention we assume that the transmission of a value v takes δ_v time units. In rule (RcvP) a receiver evolves into an active receiver $(x)_{m:v}.P$ where m is the transmitter's name and v is the value that is supposed to be received after δ_v instants of time. The process $\lfloor ?(x).P \rfloor Q$ can start a reception in the current instant of time, as $?(x).P$, or it can idle for one

Table 2 LTS - Process transitions

$$\text{(SndP)}\ \frac{-}{!\langle v\rangle.P \xrightarrow{!v} \langle v\rangle^{\delta_v}.P} \qquad \text{(RcvP)}\ \frac{-}{?(x).P \xrightarrow{?w} (x)_w.P}$$

$$\text{(RcvTO)}\ \frac{-}{\lfloor ?(x).P \rfloor Q \xrightarrow{?w} (x)_w.P} \qquad \text{(Timeout)}\ \frac{-}{\lfloor ?(x).P \rfloor Q \xrightarrow{\sigma} Q}$$

$$\text{(Nil-}\sigma\text{)}\ \frac{-}{\mathsf{nil} \xrightarrow{\sigma} \mathsf{nil}} \qquad \text{(Rcv-}\sigma\text{)}\ \frac{-}{?(x).P \xrightarrow{\sigma} ?(x).P}$$

$$\text{(Sigma)}\ \frac{-}{\sigma.P \xrightarrow{\sigma} P}$$

$$\text{(ActSnd)}\ \frac{r > 0}{\langle v\rangle^r.P \xrightarrow{\sigma} \langle v\rangle^{r-1}.P} \qquad \text{(ActRcv)}\ \frac{-}{(x)_v.P \xrightarrow{\sigma} (x)_v.P}$$

time unit evolving into Q. Rules (RcvTO) and (Timeout) model these two different behaviours, respectively. The remaining rules regards time passing. Rules (Nil-σ), (Rcv-σ), and (Sigma) are straightforward. In rule (ActSnd) the time necessary to conclude the transmission is decreased. In rule (ActRcv) the derivative does not change as a reception terminates only when the channel is sensed free. Notice that sender processes do not perform σ-actions. This is to model the maximal progress property.

We have divided the LTS for networks in two sets of rules corresponding to the two main aspects of a wireless transmission. Table 3 contains the rules to model the initial synchronisation between the sender and its neighbours. Table 4 contains the rules for modelling time passing and transmission ending.

Let us comment on the rules of Table 3. Rule (Snd) models a node starting a broadcast of message v to its neighbours in ν. By maximal progress, a node which is ready to transmit will not be delayed. Rule (Rcv) models the beginning of the reception of a message v transmitted by a station m. This happens only when the receiver is not exposed to other transmissions i.e. when the exposure indicator is equal to zero. The exposure indicator is then updated because node n will be exposed for the next δ_v instants of time. The reception will finish only when the receiver senses the channel free (see rule (Time-0) of Table 4).

Rule (RcvPar) models multiple receptions. Rule (Sync) serves to synchronise the components of a network with a broadcast transmission originating from a node m. In rule (Coll) an active receiver n is exposed to a transmission originating from a node m. This transmission gives rise to a *collision* at n. Rule (Exp) models

Table 3 LTS - Begin transmission

$$\text{(Snd)}\ \frac{P \xrightarrow{!v} A}{m[P]_t^\nu \xrightarrow{m!v} m[A]_t^\nu} \qquad \text{(Rcv)}\ \frac{m \in \nu \quad P \xrightarrow{?m:v} A}{n[P]_0^\nu \xrightarrow{m?v} n[A]_{\delta v}^\nu}$$

$$\text{(RcvPar)}\ \frac{M \xrightarrow{m?v} M' \quad N \xrightarrow{m?v} N'}{M \mid N \xrightarrow{m?v} M' \mid N'} \qquad \text{(Sync)}\ \frac{M \xrightarrow{m!v} M' \quad N \xrightarrow{m?v} N'}{M \mid N \xrightarrow{m!v} M' \mid N'}$$

$$\text{(Coll)}\ \frac{m \in \nu \quad t' := \mathsf{max}(t, \delta_v)}{n[(x)_w.P]_t^\nu \xrightarrow{m?v} n[(x)_\perp.P]_{t'}^\nu} \qquad \text{(Exp)}\ \frac{m \in \nu \quad W \neq (x)_w.P \quad t' := \mathsf{max}(t, \delta_v)}{n[W]_t^\nu \xrightarrow{m?v} n[W]_{t'}^\nu}$$

$$\text{(OutRng)}\ \frac{m \notin \nu \quad m \neq n}{n[W]_t^\nu \xrightarrow{m?v} n[W]_t^\nu} \qquad \text{(Zero)}\ \frac{-}{\mathbf{0} \xrightarrow{m?v} \mathbf{0}}$$

the exposure of a node n (which is not an active receiver) to a transmission originating from a transmitter m. In this case, n does not take part to the transmission. Notice that a node $n[?(x).P]_0^\nu$ might execute rule (Exp) instead of (Rcv). This is because a potential (synchronised) receiver might miss the synchronisation with the sender for several reasons (internal misbehaving, radio signals problems, etc). Such a situation will give rise to a failure in reception at n (see rule (RcvFail) in Table 4). Rule (OutRng) regards nodes which are out of the range of a transmission originating from a node m. Rule (Zero) is similar but regards empty networks. Rules (RcvPar) and (Sync) have their symmetric counterpart.

Let us explain the rules in Table 3 with an example.

Example 2.1 *Consider the network*

$$Net \stackrel{\text{def}}{=} k[!\langle v\rangle.?(x).P]_0^{\nu_k} \mid l[?(x).Q]_0^{\nu_l} \mid m[!\langle w\rangle]_0^{\nu_m} \mid n[?(y).R]_0^{\nu_n}$$

with the following communication topology: $\nu_k = \{l, m, \hat{l}\}$, $\nu_l = \{k, m\}$, $\nu_m = \{k, l, n, \hat{l}, \hat{m}\}$, *and* $\nu_n = \{m\}$. *There are two possible broadcast communications originating from stations* k *and* m, *respectively. Let us suppose* k *starts broadcasting. By applying rules (Snd), (Rcv), (Exp), (OutRng), (RcvPar), and (Sync)*

Table 4 LTS - Time passing/End transmission

$$\text{(Time-0)}\quad \frac{W \xrightarrow{\sigma} W' \quad W \neq (x)_w.P}{\begin{array}{c} n[W]_0^\nu \xrightarrow{\sigma} n[W']_0^\nu \\ n[(x)_w.P]_0^\nu \xrightarrow{\sigma} n[\{^w/_x\}P]_0^\nu \end{array}}$$

$$\text{(Time-t)}\quad \frac{t>0 \quad W \xrightarrow{\sigma} W' \quad W \not\xrightarrow{?v}}{n[W]_t^\nu \xrightarrow{\sigma} n[W']_{t-1}^\nu} \qquad \text{(RcvFail)}\quad \frac{t>0 \quad P \xrightarrow{?\perp} A}{n[P]_t^\nu \xrightarrow{\sigma} n[A]_{t-1}^\nu}$$

$$\text{(Zero-}\sigma\text{)}\quad \frac{-}{\mathbf{0} \xrightarrow{\sigma} \mathbf{0}} \qquad \text{(Par-}\sigma\text{)}\quad \frac{M \xrightarrow{\sigma} M' \quad N \xrightarrow{\sigma} N'}{M \mid N \xrightarrow{\sigma} M' \mid N'}$$

we have:

$$\begin{array}{rcl} Net & \xrightarrow{k!v} & k[\langle v\rangle^{\delta_v}.?(x).P]_0^{\nu_k} \mid l[(x)_{k:v}.Q]_{\delta_v}^{\nu_l} \mid m[!\langle w\rangle]_{\delta_v}^{\nu_m} \mid n[?(y).R]_0^{\nu_n} \\ & = & Net_1 \ . \end{array}$$

Now, by maximal progress, the station m must start transmitting at the same instant of time. Supposing $\delta_v < \delta_w$ we have:

$$\begin{array}{rcl} Net_1 & \xrightarrow{m!w} & k[\langle v\rangle^{\delta_v}.?(x).P]_{\delta_w}^{\nu_k} \mid l[(x)_\perp.Q]_{\delta_w}^{\nu_l} \mid m[\langle w\rangle^{\delta_w}]_{\delta_v}^{\nu_m} \mid n[(y)_{m:w}.R]_{\delta_w}^{\nu_n} \\ & = & Net_2 \ . \end{array}$$

Now, node l is exposed to a collision and its reception is doomed to fail. Notice that, although node m was already exposed when it started transmitting, node n will receive correctly the message w from m.

Let us comment on rules of Table 4. Rules (Time-0) and (Time-t) model the passage of one time unit for non-exposed and exposed nodes, respectively. In both rules the exposure indicator is decreased. Notice that for $W = !\langle v\rangle.P$ none of these two rules can be applied, as for maximal progress no transmission can be delayed. Notice also that for $W = ?(x).P$ and $t > 0$ rule (Time-t) cannot be applied. In this case, we must apply rule (RcvFail) to model a failure in reception. This may happen, for instance, when the receiver misses the preamble starting a transmission, or when a receiver wakes up in the middle of an ongoing transmission. Rule (Zero-σ) is straightforward. Rule (Par-σ) models time synchronisation. This is possible because our networks are connected. Rule (Par-σ) has its symmetric counterpart.

Table 5 LTS - Matching and recursion

$$\text{(Then)}\ \frac{n[P]^\nu_t \xrightarrow{\lambda} n[P']^\nu_{t'}}{n[[v=v]P,Q]^\nu_t \xrightarrow{\lambda} n[P']^\nu_{t'}} \qquad \text{(Else)}\ \frac{n[Q]^\nu_t \xrightarrow{\lambda} n[Q']^\nu_{t'} \quad v_1 \neq v_2}{n[[v_1=v_2]P,Q]^\nu_t \xrightarrow{\lambda} n[Q']^\nu_{t'}}$$

$$\text{(Rec)}\ \frac{n[\{\tilde{v}/\tilde{x}\}P]^\nu_t \xrightarrow{\lambda} n[P']^\nu_{t'} \quad H(\tilde{x}) \stackrel{\text{def}}{=} P}{n[H\langle\tilde{v}\rangle]^\nu_t \xrightarrow{\lambda} n[P']^\nu_{t'}}$$

Example 2.2 *Let us continue with the previous example. Let us show how the system evolves after δ_v and δ_w time units. We recall that $0 < \delta_v < \delta_w$. For simplicity let us define $\delta := \delta_w - \delta_v$:*

$$\begin{array}{lll}
Net_2 & \xrightarrow{\sigma}\xrightarrow{\delta_v} & k[?(x).P]^\nu_\delta \mid l[(x)_\perp.Q]^\nu_\delta \mid m[\langle w\rangle^\delta]^\nu_0 \mid n[(y)_{m:w}.R]^\nu_\delta \\
& \xrightarrow{\sigma} & k[(x)_\perp.P]^\nu_{\delta-1} \mid l[(x)_\perp.Q]^\nu_{\delta-1} \mid m[\langle w\rangle^{\delta-1}]^\nu_0 \mid n[(y)_{m:w}.R]^\nu_{\delta-1} \\
& \xrightarrow{\sigma}\xrightarrow{\delta-1} & k[(x)_\perp.P]^\nu_0 \mid l[(x)_\perp.Q]^\nu_0 \mid m[\mathsf{nil}]^\nu_0 \mid n[(y)_{m:w}.R]^\nu_0 \\
& \xrightarrow{\sigma} & k[\{^\perp/_x\}P]^\nu_0 \mid l[\{^\perp/_x\}Q]^\nu_0 \mid m[\mathsf{nil}]^\nu_0 \mid n[\{^{m:w}/_y\}R]^\nu_0
\end{array}$$

Notice that, after δ_v instants of time, node k will start a reception in the middle of an ongoing transmission (the transmitter being m). This will lead to a failure at k.

In the rest of the paper, the metavariable λ will range over the following labels: $m!v$, $m?v$, and σ. In Table 5 we report the obvious rules for nodes containing matching and recursive processes (we recall that only guarded recursion is allowed).

2.2 Well-formedness

The syntax presented in Table 1 allows to derive inconsistent networks, i.e. networks that do not have a realistic counterpart. Below we give a number of definitions to rule out ill-formed networks.

As network addresses are unique, we assume that there cannot be two nodes with the same name in the same network.

Definition 2.3 (Node uniqueness) *A network M is said to be* node-unique *if whenever $M \equiv M_1 \mid m[W_1]^\nu_t \mid n[W_2]^{\nu'}_{t'}$ it holds that $m \neq n$.*

We also assume network connectivity, i.e. all nodes are connected to each other, although not always directly. We recall that all nodes have the same transmission range. Formally,

Definition 2.4 (Network connectivity) *A network M is said to be* connected *if*

- *whenever $M \equiv N \mid m[W_1]_t^\nu \mid n[W_2]_{t'}^{\nu'}$ with $m \in \nu'$ it holds that $n \in \nu$;*
- *for all $m, n \in \mathsf{nds}(M)$ there is a sequence of nodes $m_1, \ldots, m_k \in \mathsf{nds}(M)$, with neighbouring $\nu_1, \ldots, \nu_k$, respectively, such that $m{=}m_1$, $n{=}m_k$, and $m_i \in \nu_{i+1}$, for $1 \leq i \leq k{-}1$.*

The next definition is about the consistency of exposure indicators of nodes. Intuitively, the exposure indicators of active senders and active receivers must be consistent with their current activity (transmission/reception). Moreover, the neighbours of active senders must have their exposure indicators consistent with the duration of the transmission.

Definition 2.5 (Exposure consistency) *A network M is said to be* exposure-consistent *if the following conditions are satisfied.*

1. *If $M \equiv N \mid m[(x)_v.P]_t^\nu$, with $v \neq \bot$, then $0 \leq t \leq \delta_v$.*
2. *If $M \equiv N \mid m[\langle v \rangle^r.P]_t^\nu$, then $r \leq \delta_v$.*
3. *If $M \equiv N \mid m[\langle v \rangle^r.P]_t^\nu \mid n[W]_{t'}^{\nu'}$, with $m \in \nu'$, then $0 < r \leq t'$.*
4. *Let $M \equiv N \mid n[W]_t^\nu$ with $t{>}0$. If $\mathsf{active}(k, N) \neq t$ for all k in $\nu \cap \mathsf{actsnd}(N)$, then there is k' in $\nu \backslash \mathsf{nds}(N)$ such that whenever $N \equiv N' \mid l[W']_{t'}^{\nu'}$, with $k' \in \nu'$, then $t' \geq t$.*

The next definition is about the consistency of transmitting stations. The first and the second part are about successful transmissions, while the third part is about collisions.

Definition 2.6 (Transmission consistency) *A network M is said to be* transmission-consistent *if the following conditions are satisfied.*

1. *If $M \equiv N \mid n[(x)_v.Q]_t^\nu$ and $v \neq \bot$, then $\mid \mathsf{actsnd}(N) \cap \nu \mid \leq 1$.*
2. *If $M \equiv N \mid m[\langle w \rangle^r.P]_t^\nu \mid n[(x)_v.Q]_{t'}^{\nu'}$, with $m \in \nu'$ and $v \neq \bot$, then (i) $v = m{:}w$, and (ii) $r = t'$.*

3. If $M \equiv N \mid n[(x)_v.P]^{\nu}_t$, *with* $\mid \mathsf{actsnd}(N) \cap \nu \mid > 1$, *then* $v = \bot$.

Definition 2.7 (Well-formedness) *A network* M *is said to be* well-formed *if it is node-unique, connected, exposure-consistent, and transmission-consistent.*

In the sequel, we will work only with well-formed networks.

3 Properties

We start proving three desirable time properties of TCWS: time determinism, patience, and maximal progress. We then show that our LTS preserves network well-formedness.

Theorem 3.1 formalises the determinism nature of time passing: a network can reach at most one new state by executing the action σ.

Theorem 3.1 (Time Determinism) *Let* M *be a well-formed network. If* $M \xrightarrow{\sigma} M'$ *and* $M \xrightarrow{\sigma} M''$ *then* M' *and* M'' *are syntactically the same.*

Proof By induction on the length of the proof of $M \xrightarrow{\sigma} M'$. □

In [17, 33], the maximal progress property says that processes communicate as soon as a possibility of communication arises. However, unlike [17, 33], in our calculus message transmission requires a positive amount of time. So, we generalise the property saying that transmissions cannot be delayed.

Theorem 3.2 (Maximal Progress) *Let* M *be a well-formed network. If there is* N *such that* $M \xrightarrow{m!v} N$ *then* $M \xrightarrow{\sigma} M'$ *for no network* M'.

Proof Because sender nodes cannot perform σ-actions. □

The last time property is patience. In [17, 33] patience guarantees that a process will wait indefinitely until it can communicate. In our setting, this means that if no transmission can start then it must be possible to execute a σ-action to let time pass.

Theorem 3.3 (Patience) *Let* M *be a well-formed network. If* $M \xrightarrow{m!v} M'$ *for no network* M' *then there is a network* N *such that* $M \xrightarrow{\sigma} N$.

Proof By contradiction and then by induction on the structure of M. □

Finally, we prove that network well-formedness is preserved at runtime. In particular, the preservation of exposure- and transmission-consistency are the more interesting and delicate results.

Theorem 3.4 (Subject reduction) *If M is a well-formed network, and $M \xrightarrow{\lambda} M'$ for some label λ and network M', then M' is well-formed as well.*

Proof By transition induction. □

4 A case study: the Carrier Sense Multiple Access scheme

The *Carrier Sense Multiple Access* (CSMA) scheme [19] is a widely-used MAC level protocol in which a device senses the channel before transmitting. More precisely, if the channel is sensed free, the sender starts transmitting immediately (i.e. in the next instant of time [3]); if the channel is busy (i.e. some other station is transmitting) the device keeps listening the channel until it becomes idle and then starts transmitting immediately. This strategy is called *1-persistent* CSMA. More generally, in a *p-persistent* CSMA strategy (where p is a probability) the sender transmits with probability p, and waits for the next available time slot, with probability $1 - p$.

In our calculus, we can easily model the 1-persistent CSMA scheme using receivers with timeout where the sender process $!\langle v\rangle.P$ is replaced by the process defined below:

$$!!\langle v\rangle.P \stackrel{\text{def}}{=} \lfloor ?(x).!\langle v\rangle.P \rfloor !\langle v\rangle.P \ .$$

The next example shows how 1-persistent CSMA affects the behaviour of a wireless system. Let us consider the network:

$$Net \stackrel{\text{def}}{=} k[!!\langle v\rangle.?(x).P]_0^{\nu_k} \mid l[?(x).Q]_0^{\nu_l} \mid m[\sigma.!!\langle w\rangle]_0^{\nu_m} \mid n[?(y).R]_0^{\nu_n}$$

with the following communication topology: $\nu_k = \{l, m, \hat{l}\}$, $\nu_l = \{k, m\}$, $\nu_m = \{k, l, n, \hat{l}, \hat{m}\}$, and $\nu_n = \{m\}$. Here, node k senses the channel free and, according to the CSMA scheme, in the next instant of time it will start transmitting. Thus,

$$\begin{array}{rcl} Net & \xrightarrow{\sigma} & k[!\langle v\rangle.?(x).P]_0^{\nu_k} \mid l[?(x).Q]_0^{\nu_l} \mid m[!!\langle w\rangle]_0^{\nu_m} \mid n[?(y).R]_0^{\nu_n} \\ & = & Net_1 \ . \end{array}$$

[3] We recall that in wireless systems channels are half-duplex.

In Net_1, node m it is currently listening the channel to check whether it is free. By applying rules (Snd), (Rcv), (Exp), (OutRng), (RcvPar), and (Sync) node k can start transmitting:

$$\begin{array}{rcl} Net_1 & \xrightarrow{k!v} & k[\langle v\rangle^{\delta_v}.?(x).P]_0^{\nu_k} \mid l[(x)_{k:v}.Q]_{\delta_v}^{\nu_l} \mid m[(x)_{k:v}.!\langle w\rangle]_{\delta_v}^{\nu_m} \mid n[?(y).R]_0^{\nu_n} \\ & = & Net_2 \ . \end{array}$$

Now, since k has already started its transmission, node m senses the channel busy and it must wait until the channel becomes free. Notice that in this manner there are no collisions at l and/or k. In fact, after δ_v instants of time we have:

$$\begin{array}{rcl} Net_2 & \xrightarrow{\sigma}^{\delta_v} & k[?(x).P]_0^{\nu_k} \mid l[(x)_{k:v}.Q]_0^{\nu_l} \mid m[(x)_{k:v}.!\langle w\rangle]_0^{\nu_m} \mid n[?(y).R]_0^{\nu_n} \\ & \xrightarrow{\sigma} & k[?(x).P]_0^{\nu_k} \mid l[\{^{k:v}/_x\}Q]_0^{\nu_l} \mid m[!\langle w\rangle]_0^{\nu_m} \mid n[?(y).R]_0^{\nu_n} \\ & = & Net_3 \end{array}$$

where node l has successfully received value v from k. Notice that after δ_v instants of time node m senses the channel free, and by maximal progress it will start transmitting in the next instant of time.

Notice that, using a CSMA scheme, there is always a chance of stations transmitting at the same time, caused by the fact that different stations sensed the medium free and decided to transmit at once. As an example, consider the network:

$$Net' \stackrel{\text{def}}{=} k[!!\langle v\rangle.?(x).P]_0^{\nu_k} \mid l[?(x).Q]_0^{\nu_l} \mid m[!!\langle w\rangle]_0^{\nu_m} \mid n[?(y).R]_0^{\nu_n}$$

with the same communication topology as before. In this scenario, both nodes k and m want to start transmitting. And since both of them sense the channel free, they will start transmitting in the next instant of time. Thus, assuming $\delta_v < \delta_w$, we have:

$$\begin{array}{rcl} Net' & \xrightarrow{\sigma} & k[!\langle v\rangle.?(x).P]_0^{\nu_k} \mid l[?(x).Q]_0^{\nu_l} \mid m[!\langle w\rangle]_0^{\nu_m} \mid n[?(y).R]_0^{\nu_n} \\ & \xrightarrow{k!v} & k[\langle v\rangle^{\delta_v}.?(x).P]_0^{\nu_k} \mid l[(x)_{k:v}.Q]_{\delta_v}^{\nu_l} \mid m[!\langle w\rangle]_{\delta_v}^{\nu_m} \mid n[?(y).R]_0^{\nu_n} \\ & \xrightarrow{m!w} & k[\langle v\rangle^{\delta_v}.?(x).P]_{\delta_w}^{\nu_k} \mid l[(x)_{\perp}.Q]_{\delta_w}^{\nu_l} \mid m[\langle w\rangle^{\delta_w}]_{\delta_v}^{\nu_m} \mid n[(y)_{m:w}.R]_{\delta_w}^{\nu_n} \ . \end{array}$$

In this situation, node l is exposed to a collision caused by the two transmissions.

Notice that, the CSMA scheme is not always a good idea. Let us consider, for instance, the previous network Net where nodes l and m are not neighbours anymore, that is $\nu_l = \{k\}$ and $\nu_m = \{k, n, \hat{l}, \hat{m}\}$. Now, suppose that m wants to

send a message to n. Then, the CSMA scheme delays the transmission without any reason, only because m is exposed to the transmission originating from k. This is a well-known problem, introduced by CSMA, called *exposed terminal problem*.

The CSMA scheme suffers another well-known problem called *hidden terminal problem*. This happens when two transmitters sense the channel free, because they are not in each other's transmission cell, and start transmitting causing a collision to a third node lying in the transmission cells of both. As an example, you can consider, for instance, the previous network Net with the following communication topology: $\nu_k = \{l, \hat{l}\}$, $\nu_l = \{k, m\}$, $\nu_m = \{l, n, \hat{l}, \hat{m}\}$, and $\nu_n = \{m\}$. In this case, both transmissions at k and m will fire causing (after two instants of time) an interference at l.

In unicast communications, to reduce the number of collisions due to the hidden terminal problem, the CSMA scheme may be used together with a CA (Collision Avoidance) protocol. In this protocol, before transmitting the message, two special packets (RTS/CTS) are sent to reserve the channel [19]. On one hand this technique reduce the number of collisions, on the other hand the transmission of extra data may drastically reduce the performances of the network. Moreover, the CSMA/CA protocol does not help for broadcast communication.

5 Observational semantics

In this section we propose a notion of timed behavioural equivalence for our wireless networks. Our starting point is Milner and Sangiorgi's barbed congruence [27], a standard contextually-defined program equivalence. Intuitively, two terms are barbed congruent if they have the same *observables*, in all possible contexts, under all possible *evolutions*. The definition of barbed congruence strongly relies on two crucial concepts: a reduction semantics to describe how a system evolves, and a notion of observable which says what the environment can observe in a system.

From the operational semantics given in Section 2.1 it should be clear that a wireless network evolves transmitting messages. Notice that a transmission in a network does not require any synchronisation with the environment. Thus, we can define the reduction relation $\rightarrowtriangle$ between networks using the following inference rule

$$\text{(Red)}\ \frac{M \xrightarrow{m!v} N}{M \rightarrowtriangle N}\ .$$

We write $\rightarrowtriangle^\star$ for the reflexive and transitive closure of $\rightarrowtriangle$.

Now, let us focus on the definition of an appropriate notion of observable. In our calculus, as in CCS [25] and in π-calculus [26], we have both transmission and reception of messages. However, in broadcast calculi only the transmission of messages may be observed [34, 23]. In fact, an observer cannot detect whether a given node actually receives a broadcast value. In particular, if the node $m[!\langle v\rangle.P]_t^\nu$ evolves into $m[\langle v\rangle^r.P]_t^\nu$ we do not know whether some of the neighbours have actually synchronised for receiving the message v. On the other hand, if a *non-exposed* node $n[?(x).P]_0^\nu$ evolves into $n[(x)_{m:v}.P]_t^\nu$, then we can be sure that some node in ν has started transmitting. Notice that a node n can certify the reception of a message v from a transmitter m only if it receives the whole message without collisions.

Following Milner and Sangiorgi [27] we use the term "barb" as synonymous of observable.

Definition 5.1 (Barbs) *Let M be a well-formed network. We write $M \downarrow_n$, if $M \equiv N \mid m[\langle v\rangle^r.P]_t^\nu$, for some m, v, r, P, t and ν, such that $n \in \nu$ and $n \notin \mathsf{nds}(N)$. We write $M \Downarrow_n$ if there is M' such that $M \twoheadrightarrow^\star M' \downarrow_n$.*

The barb $M \Downarrow_n$ says that there is a transmission at M reaching the node n of the environment. The observer can easily detect such a transmission placing a receiver with timeout at n. Say, something like $n[\lfloor ?(x).\mathbf{0}\rfloor !\langle w\rangle.\mathbf{0}]_t^\nu$, where $M \mid n[\lfloor ?(x).\mathbf{0}\rfloor !\langle w\rangle.\mathbf{0}]_t^\nu$ is well-formed, and $f \in \nu$, for some fresh name f. In this manner, if n is currently exposed to a transmission then, after a σ-action, the fresh barb at f is definitely lost. One may wonder whether the barb should mention the name m of the transmitter, which is usually recorded in some specific field of the packets. Notice that, in general, due to communication collisions, the observer may receive incomprehensible packets without being able to identify the transmitter. In fact, if $M \downarrow_n$ there might be several nodes in M which are currently transmitting to n. So, in our opinion, in our setting, it does not make sense to put the name of the transmitter in the barb.

Now, everything is in place to define our timed notion of barbed congruence. In the sequel, we write $\mathcal{R}$ to denote binary relations over well-formed networks.

Definition 5.2 (Barb preserving) *A relation $\mathcal{R}$ is said to be* barb preserving *if whenever $M\ \mathcal{R}\ N$ it holds that $M \downarrow_n$ implies $N \Downarrow_n$.*

Definition 5.3 (Reduction closure) *A relation $\mathcal{R}$ is said to be* reduction-closed *if $M\ \mathcal{R}\ N$ and $M \twoheadrightarrow M'$ imply there is N' such that $N \twoheadrightarrow^\star N'$ and $M'\ \mathcal{R}\ N'$.*

As we are interested in weak behavioural equivalences, the definition of reduction closure is given in terms of weak reductions.

Definition 5.4 (σ-closure) *A relation $\mathcal{R}$ is said to be* σ-closed *if $M\ \mathcal{R}\ N$ and $M \xrightarrow{\sigma} M'$ imply there is a network N' such that $N \twoheadrightarrow^* \xrightarrow{\sigma} \twoheadrightarrow^* N'$ and $M'\ \mathcal{R}\ N'$.*

When comparing two networks M and N, time must pass in the same manner for M and N.

Definition 5.5 (Contextuality) *A relation $\mathcal{R}$ is said* contextual *if $M\ \mathcal{R}\ N$, for M and N well-formed, implies $M \mid O\ \mathcal{R}\ N \mid O$ for all networks O such that $M \mid O$ and $N \mid O$ are well-formed.*

Finally, everything is in place to define timed reduction barbed congruence.

Definition 5.6 (Timed reduction barbed congruence) Timed reduction barbed congruence*, written $\cong$, is the largest symmetric relation over well-formed networks which is barb preserving, reduction-closed, σ-closed, and contextual.*

6 A bisimulation proof method

The definition of timed reduction barbed congruence is simple and intuitive. However, due to the universal quantification on parallel contexts, it may be quite difficult to prove that two terms are barbed congruent. Simpler proof techniques are based on labelled bisimilarities. In this section, we propose an appropriate notion of bisimulation between networks. As a main result, we prove that our labelled bisimilarity is a proof-technique for timed reduction barbed congruence.

First of all we have to distinguish between transmissions which may be observed and transmissions which may not be observed.

$$\text{(Shh)}\ \frac{M \xrightarrow{m!v} N \quad \mathsf{ngh}(m,M)\subseteq\mathsf{nds}(M)}{M \xrightarrow{\tau} N} \qquad \text{(Out)}\ \frac{M \xrightarrow{m!v} N \quad \nu:=\mathsf{ngh}(m,M)\setminus\mathsf{nds}(M)\neq\emptyset}{M \xrightarrow{m!v\triangleright\nu} N}$$

Rule (Shh) models transmissions that cannot be detected by the environment. This happens if none of the potential receivers is in the environment. Notice that, although there is no explicit rule, τ-actions propagate through parallel composition.

Lemma 6.1 *If $M \xrightarrow{\tau} M'$ then $M \mid N \xrightarrow{\tau} M' \mid N$ and $N \mid M \xrightarrow{\tau} N \mid M'$.*

Rule (Out) models a transmission of a message that may be potentially received by the nodes ν of the environment. Notice that this transmission can be really observed at some node $n \in \nu$ only if no collisions arise at n during the transmission of v.

In the sequel, we use the metavariable α to range over the following actions: τ, σ, $m?v$, and $m!v\triangleright\nu$. Since we are interested in *weak behavioural equivalences*, that abstract over τ-actions, we introduce a standard notion of weak action: $\Rightarrow$ denotes the reflexive and transitive closure of $\stackrel{\tau}{\longrightarrow}$; $\stackrel{\alpha}{\Longrightarrow}$ denotes $\Rightarrow\stackrel{\alpha}{\longrightarrow}\Rightarrow$; $\stackrel{\hat{\alpha}}{\Longrightarrow}$ denotes $\Rightarrow$ if $\alpha=\tau$ and $\stackrel{\alpha}{\Longrightarrow}$ otherwise.

Definition 6.2 (Bisimilarity) *A relation $\mathcal{R}$ over well-formed networks is a* simulation *if $M\ \mathcal{R}\ N$ implies that*

- $\mathsf{nds}(M)=\mathsf{nds}(N)$
- *whenever $M\stackrel{\alpha}{\longrightarrow}M'$ there is N' such that $N\stackrel{\hat{\alpha}}{\Longrightarrow}N'$ and $M'\ \mathcal{R}\ N'$.*

A relation $\mathcal{R}$ is called bisimulation *if both $\mathcal{R}$ and its converse are simulations. We say that M and N are* bisimilar*, written $M\approx N$, if there is some bisimulation $\mathcal{R}$ such that $M\ \mathcal{R}\ N$.*

The requirement that two bisimilar networks must have the same nodes is quite reasonable. Technically, this is necessary to prove that the bisimilarity is a congruence.

In order to prove that our labelled bisimilarity implies timed reduction barbed congruence we have to show its contextuality.

Theorem 6.3 ($\approx$ is contextual) *Let M and N be two well-formed networks such that $M\approx N$. Then $M\mid O\approx N\mid O$ for all networks O such that $M\mid O$ and $N\mid O$ are well-formed.*

Proof See the Appendix. □

Theorem 6.4 (Soundness) *Let* ngh *be a neighbouring function and M and N two well-formed networks wrt* ngh *such that $M\approx N$. Then $M\cong N$.*

Proof We have to prove that the labelled bisimilarity is contextual, barb preserving, reduction- and σ-closed. Contextuality follows from Theorem 6.3. Reduction and σ-closure follow by definition. As to barb preservation we reason by contradiction, if $M\downarrow_n$ we can choose $O\stackrel{\text{def}}{=}n[\lfloor?(x).\mathbf{0}\rfloor!\langle w\rangle.\mathbf{0}]^{\nu}_{t}$ such that $M\mid O$ and $N\mid O$ are well-formed, and $f\in\nu$, for some fresh name f. Since $M\downarrow_n$ the network $M\mid O$ will never (even in the future) perform an output action $n!w\triangleright\nu$. On the other hand, if $N\not\downarrow_n$ we would have $N\mid O\stackrel{\sigma}{\Longrightarrow}\stackrel{n!w\triangleright\nu}{\Longrightarrow}$. However, by Theorem 6.3 we have $M\mid O\approx N\mid O$. So, it must be $N\Downarrow_n$. □

In Theorem 6.5, we report a number of algebraic properties on well-formed networks that can be proved using our bisimulation proof-technique. The first and the second law show different but equivalent nodes that do not interact with the rest of the network. The third law is about exposed and sleeping nodes. The forth law is about successful reception. Here, node n will receive correctly because all its neighbours will not interfere during the current transmission. The fifth and the sixth law are about collisions: in both cases the transmission at m will cause a collision at n. The seventh law tells about the blindness of receivers exposed to collisions. In particular, if all neighbours of a transmitter are exposed, then the content of the transmission is irrelevant as all recipients will fail. Only the duration of the transmission may be important as the exposure indicators of the neighbours may change.

Theorem 6.5

1. $n[\mathsf{nil}]_t^\nu \approx n[Sleep]_t^\nu$, *where* $Sleep \stackrel{\text{def}}{=} \sigma.Sleep$.
2. $n[\mathsf{nil}]_t^\nu \approx n[P]_t^\nu$, *if* P *does not contain sender processes.*
3. $n[\sigma^r.P]_s^\nu \approx n[\sigma^r.P]_t^\nu$ *if* $s \leq r$ *and* $t \leq r$.
4. $m[\langle v\rangle^r.P]_t^\nu \mid n[(x)_{m:v}.Q]_r^{\nu'} \mid M \approx m[\langle v\rangle^r.P]_t^\nu \mid n[\sigma^r.\{^{m:v}/_x\}Q]_r^{\nu'} \mid M$, *if* $m \in \nu'$ *and for all* $n \in \nu' \setminus m$ *it holds that* $M \equiv n[\sigma^s.R]_{t_n}^{\nu_n} \mid M'$, *with* $s \geq r$.
5. $m[!\langle v\rangle.P]_s^\nu \mid n[(x)_w.Q]_t^{\nu'} \approx m[!\langle v\rangle.P]_s^\nu \mid n[(x)_\perp.Q]_t^{\nu'}$, *if* $m \in \nu'$.
6. $m[\langle v_1\rangle^r.!\langle v_2\rangle.P]_s^\nu \mid n[(x)_w.Q]_t^{\nu'} \approx m[\langle v_1\rangle^r.!\langle v_2\rangle.P]_s^\nu \mid n[(x)_\perp.Q]_t^{\nu'}$, *if* $m \in \nu'$.
7. $m[!\langle v\rangle.P]_t^\nu \mid N \approx m[!\langle w\rangle.P]_t^\nu \mid N$, *if* $\delta_v = \delta_w$, *and for all* $n \in \nu$ *it holds that* $N \equiv n[W]_{t'}^{\nu'} \mid N'$, *with* $t' > 0$.

Proof By exhibiting the appropriate bisimulations. Let us prove, for instance, Laws 5 and 7. Let us start with Law 5. For convenience, let us define:

- $A \stackrel{\text{def}}{=} m[!\langle v\rangle.P]_s^\nu \mid n[(x)_w.Q]_t^{\nu'}$
- $B \stackrel{\text{def}}{=} m[!\langle v\rangle.P]_s^\nu \mid n[(x)_\perp.Q]_t^{\nu'}$.

Let

$$\mathcal{S} \stackrel{\text{def}}{=} \{(A, B) \mid \text{ for all } s \text{ and } t\} \cup Id$$

where Id is the identity relation over network terms. We prove that $\mathcal{S}$ is a bisimulation. We proceed by case analysis on the possible transitions of A. Notice that by maximal progress, no σ-actions may be performed.

- If $A \xrightarrow{h?v'} A'$. The most interesting case is when $h \in \nu \cap \nu'$. In this case, by an application of rules (Coll), (Exp), and (RcvPar) we have $A' = m[!\langle v\rangle.P]^{\nu}_{s'} \mid n[(x)_{\perp}.Q]^{\nu'}_{t'}$, where $t' = \max(t, \delta_{v'})$ and $s' = \max(s, \delta_{v'})$. Similarly, we have $B \xrightarrow{h?v'} A'$ and we are done.
- If $A \xrightarrow{m!v\triangleright\hat{\nu}} A'$, with $\hat{\nu} = \nu \setminus \{n\} \neq \emptyset$, then since $m \in \nu'$, by an application of rules (Snd), (Coll), (Sync), and (Out) it follows that $A' = m[\langle v\rangle^{\delta_v}.P]^{\nu}_{s} \mid n[(x)_{\perp}.Q]^{\nu'}_{t'}$ with $t' = \max(t, \delta_v)$. Similarly, we have $B \xrightarrow{m!v\triangleright\hat{\nu}} A'$ and we are done.
- If $A \xrightarrow{\tau} A'$, because $A \xrightarrow{m!v} A'$ and $\nu = \{n\}$. This case is similar to the previous one.

As regards the proof of Law 7, let us define:

- $A_1 \stackrel{\text{def}}{=} m[!\langle v\rangle.P]^{\nu}_{t} \mid N$, where for all $n \in \nu$ it holds that $N \equiv n[W]^{\nu'}_{t'} \mid N'$, with $t' > 0$
- $B_1 \stackrel{\text{def}}{=} m[!\langle w\rangle.P]^{\nu}_{t} \mid N$, where for all $n \in \nu$ it holds that $N \equiv n[W]^{\nu'}_{t'} \mid N'$, with $t' > 0$
- $A_2 \stackrel{\text{def}}{=} m[\langle v\rangle^{r}.P]^{\nu}_{t} \mid N$, with $r \leq \delta_v$, where for all $n \in \nu$ it holds that $N \equiv n[W]^{\nu'}_{t'} \mid N'$, with $t' \geq r$
- $B_2 \stackrel{\text{def}}{=} m[\langle v\rangle^{r}.P]^{\nu}_{t} \mid N$, with $r \leq \delta_w$, where for all $n \in \nu$ it holds that $N \equiv n[W]^{\nu'}_{t'} \mid N'$, with $t' \geq r$

where $\delta_v = \delta_w$. Now, let

$$\mathcal{S} \stackrel{\text{def}}{=} \{(A_1, B_1) : \text{ for all } P, t, \nu, \ldots\} \cup \{(A_2, B_2) : \text{ for all } P, t, \nu, \ldots)\} \cup Id$$

where Id is the identity relation between network terms. We prove that $\mathcal{S}$ is a bisimulation. We proceed by case analysis on the possible transitions.

- Let us examine the most interesting transitions of A_1. The reasoning for the other transitions of A_1 is simpler. Notice that by maximal progress the term A_1 cannot perform σ-actions.
  - Let $A_1 \xrightarrow{\tau} A_2 = m[\langle v\rangle^{\delta_v}.P]^{\nu}_{t} \mid \hat{N}$, because $A_1 \xrightarrow{m!v} A_2$ by an application of rule (Shh). This is possible only by an application of rule (Sync) with
    * $m[!\langle v\rangle.P]^{\nu}_{t} \xrightarrow{m!v} m[\langle v\rangle^{\delta_v}.P]^{\nu}_{t}$

* $N \xrightarrow{m?v} \hat{N}$, where if $n \in \nu$ then $\hat{N} \equiv n[\hat{W}]^{\nu'}_{\hat{t}} \mid \hat{N}'$, with $\hat{t} \geq \delta_v$ (by definition of rules (Coll) and (Exp)).

Notice that since all nodes in $\nu \cap \mathsf{nds}(N)$ are exposed, it follows that if $\hat{W}$ is an active receiver then it will be of the form $(x)_{\perp}.P$, for some P. Now, $A_2 \xrightarrow{\tau} B_2 = m[\langle w \rangle^{\delta_w}.P]^{\nu}_{t} \mid \hat{\hat{N}}$, because $A_2 \xrightarrow{m!v} B_2$ by an application of rule (Shh). This is possible only by an application of rule (Sync) with

* $m[!\langle w \rangle.P]^{\nu}_{t} \xrightarrow{m!w} m[\langle w \rangle^{\delta_w}.P]^{\nu}_{t}$
* $N \xrightarrow{m?w} \hat{\hat{N}}$, where if $n \in \nu$ then $\hat{\hat{N}} \equiv n[\hat{\hat{W}}]^{\nu'}_{\hat{\hat{t}}} \mid \hat{\hat{N}}'$, with $\hat{\hat{t}} \geq \delta_v$ (by definition of rules (Coll) and (Exp)).

Again, since all nodes in $\nu \cap \mathsf{nds}(N)$ are exposed, it follows that if $\hat{\hat{W}}$ is an active receiver then it will be of the form $(x)_{\perp}.P$, for some P. Moreover, since $\delta_v = \delta_w$ it follows $\hat{t} = \hat{\hat{t}}$. As a consequence, $\hat{N} = \hat{\hat{N}}$ and $(A_2, B_2) \in \mathcal{S}$.

- Let us examine the most interesting transitions of A_2. The reasoning for the other transitions is simpler.
  - Let $A_2 \xrightarrow{\sigma} A'_2 = m[\langle v \rangle^{r-1}.P]^{\nu}_{t \ominus 1} \mid \hat{N}$ by an application of rule (Par-σ) because
    * $m[\langle v \rangle^{r}.P]^{\nu}_{t} \xrightarrow{\sigma} m[\langle v \rangle^{r-1}.P]^{\nu}_{t \ominus 1}$
    * $N \xrightarrow{\sigma} \hat{N}$.

    In this case we have $B_2 \xrightarrow{\sigma} B'_2 = m[\langle w \rangle^{r-1}.P]^{\nu}_{t \ominus 1} \mid \hat{N}$. Now, independently whether $r > 1$ or not we have $(A'_2, B'_2) \in \mathcal{S}$.

□

7 Future and related work

We have proposed a timed process calculus for IBBS networks with a focus on communication collisions. To our knowledge this is the first timed process calculus for wireless networks. In our model, time and collisions are treated in a completely *orthogonal* way.

Now, we give an overview of what we believe are possible future works.

In TCWS we have assumed the presence of a unique channel. However, new techniques have been developed in the last years to provide several virtual channels. The most known techniques are *Frequency Division Multiplexing* (FDM), in

which the signal is splitted into many narrow bands, and *Time Division Multiplexing* (TDM), in which the time domain is divided into several recurrent timeslots of fixed lenght, one for each sub-channel. A generalisation of TCWS with multiple channels (à la CCS) is straightforward.

For simplicity, in TCWS we rely on a static network topology. As a consequence, our results mainly applies to *stationary networks*. Notice that movement is not relevant in important classes of wireless systems, most notably *sensor networks* (not all sensor networks are stationary, but the stationary case is predominant). However, we believe it is possible to adopt the techniques developed in [12, 13] to allow disciplined forms of mobility in TCWS, where neighbouring relations may change provided that the network connectivity is mantained. This will be one of the next directions of our research.

In Section 4, we have seen that the CSMA scheme (even in its p-persistent form) suffers of several problems such as the exposed terminal problem and the hidden terminal problem. Clearly, in a broadcast environment where there exists no direct mechanism to infer the loss of information owing to collisions, it is important to indirectly and accurately determine the *probability* of packet collisions. We believe that our calculus represents a solid basis to develop a probabilistic calculus where transmitters start transmitting with a certain probability p (independently whether the channel is free) and with probability $1 - p$ waits before transmitting. The goal would be that of developping verification techniques such as *probabilistic model checking* [20] to guarantee the absence of collisions with a certain probability. This will be one of the directions of our research.

Last but not least, we believe that our timed calculus can be used as a basis to develop *trust models* for wireless systems. Trust establishment in ad hoc networks is an open and challenging field. In fact, without a centralised trusty authority it is not obvious how to build and maintain trust. Nevertheless, the notion of time seems to be important to represent credentials' expiration.

Let us examine now the most relevant related works.

We start with the literature on process calculi for wireless systems. Nanz and Hankin [30] have introduced a calculus for Mobile Wireless Networks (CBS$^\sharp$), relying on graph representation of node localities. The main goal of the paper is to present a framework for specification and security analysis of communication protocols for mobile wireless networks. Merro [23] has proposed a process calculus for Mobile Ad Hoc Networks with a labelled characterisation of reduction barbed congruence. Godskesen [14] has proposed a calculus for mobile ad hoc networks (CMAN). The paper proves a characterisation of reduction barbed congruence in terms of a contextual bisimulation. It also contains a formalisation of an attack on the cryptographic routing protocol ARAN. Singh, Ramakrishnan, and Smolka [37] have proposed the ω-calculus, a conservative extension of the π-calculus. A

key feature of the ω-calculus is the separation of a node's communication and computational behaviour from the description of its physical transmission range. The authors provide a labelled transition semantics and a bisimulation in "open" style. The ω-calculus is then used for modelling the AODV routing protocol. Ghassemi et al. [12] have proposed a process algebra for mobile ad hoc networks (RBPT) where, topology changes are implicitly modelled in the (operational) semantics rather than in the syntax. The authors propose a notion of bisimulation for networks parameterised on a set of topology invariants that must be respected by equivalent networks. This work in then refined in [13] where the authors propose an equational theory for an extension of RBPT. All the previous calculi abstract from the presence of interferences. Mezzetti and Sangiorgi [24] have instead proposed the CWS calculus, a lower level calculus to describe interferences in wireless systems. In their LTS there is a separation between transmission beginning and transmission ending. Our work was definitely inspired by [24].

None of the calculi mentioned above deals with time, although there is an extensive literature on timed process algebra. From a purely syntactic point of view, the earliest proposals are extensions of the three main process algebras, ACP, CSP and CCS. For example, [2] presents a real-time extension of ACP, [35] contains a denotational model for a timed extension of CSP, while CCS is the starting point for [29]. In [2] and [35] time is real-valued, and at least semantically, associated directly with actions. The other major approach to representing time is to introduce special actions to model the passage of time, which the current paper shares with [16, 5, 29, 31] and [40, 41], although the basis for all those proposals may be found in [7]. The current paper shares many of the assumptions of the languages presented in these papers. For example, all the papers above assume that actions are instantaneous and only the extension of ACP presented in [16] does not incorporate time determinism; however maximal progress is less popular and patience is even rarer.

More recent works on timed process algebra include the following papers. Aceto and Hennessy [1] have presented a simple process algebra where time emerges in the definition of a *timed observational equivalence*, assuming that beginning and termination of actions are distinct events which can be observed. Hennessy and Regan [17] have proposed a timed version of CCS enjoying time determinism, maximal progress, and patience. Our action σ takes inspiration from theirs. The authors have developed a semantic theory based on testing and characterised in terms of a particular kind of ready traces. Prasad [33] has proposed a timed variant of his CBS [32], called TCBS. In TCBS a time out can force a process wishing to speak to remain idle for a specific interval of time; this corresponds to have a priority. TCBS also assumes time determinism and maximal progress. Corradini et al. [9] deal with *durational actions* proposing

a framework relying on the notions of reduction and observability to naturally incorporate timing information in terms of process interaction. Our definition of timed reduction barbed congruence takes inspiration from theirs. Corradini and Pistore [10] have studied durational actions to describe and reason about the performance of systems. Actions have lower and upper time bounds, specifying their possible different durations. Their *time equivalence* refines the untimed one. Baeten and Middelburg [3] have proposed several timed process algebras treated in a common framework, and related by embeddings and conservative extensions relations. These process algebras, $\mathrm{ACP}^{\mathrm{sat}}$, $\mathrm{ACP}^{\mathrm{srt}}$, $\mathrm{ACP}^{\mathrm{dat}}$ and $\mathrm{ACP}^{\mathrm{drt}}$, allow the execution of two or more actions consecutively at the same point in time, separate the execution of actions from the passage of time, and consider actions to have no duration. The process algebra $\mathrm{ACP}^{\mathrm{sat}}$ is a real-time process algebra with absolute time, $\mathrm{ACP}^{\mathrm{srt}}$ is a real-time process algebra with relative time. Similarly, $\mathrm{ACP}^{\mathrm{dat}}$ and $\mathrm{ACP}^{\mathrm{drt}}$ are discrete-time process algebras with absolute time and relative time, respectively. In these process algebra the focus is on unsuccessful termination or deadlock. In [4] Baeten and Reniers extend the framework of [3] to model successful termination for the relative-time case. Laneve and Zavattaro [21] have proposed a timed extension of π-calculus where time proceeds asynchronously at the network level, while it is constrained by the local urgency at the process level. They propose a timed bisimilarity whose discriminating is weaker when local urgency is dropped.

Acknowledgements We thank Sebastian Nanz for a preliminary discussion on timed calculi for wireless networks. Davide Quaglia for insightful discussions on the IEEE 802.11 standard. Many thanks to Matthew Hennessy for his precious comments on a early draft of the paper. Many thanks to Andrea Cerone for suggesting to use the receiver with timeout to model the CSMA protocol.

References

[1] L. Aceto and M. Hennessy. Towards action-refinement in process algebras. *Information and Computation*, 103(2):204–269, 1993.

[2] J. Baeten and J. Bergstra. Real Time Process Algebra. *Formal Aspects of Computing*, 3(2):142–188, 1991.

[3] J. Baeten and C. Middelburg. *Process Algebra with Timing*. EATCS Series. Springer-Verlag, 2002.

[4] J. C. M. Baeten and M. A. Reniers. Timed Process Algebra (With a Focus on Explicit Termination and Relative-Timing). In *SFM*, volume 3185 of *Lecture Notes in Computer Science*, pages 59–97. Springer-Verlag, 2004.

[5] J.C.M. Baeten and J.A. Bergstra. Discrete time process algebra. *Formal Aspects of Computing*, 8(2):188–208, 1996.

[6] J.A. Bergstra and J.W. Klop. Process algebra for synchronous communication. *Information and Computation*, 60:109–137, 1984.

[7] G. Berry and L. Cosserat. The ESTEREL Synchronous Programming Language and its Mathematical Semantics. Technical Report 842, INRIA, Sophia-Antipolis, 1988.

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

[9] F. Corradini, G. Ferrari, and M. Pistore. On the semantics of durational actions. *Theoretical Computer Science*, 269(1-2):47–82, 2001.

[10] F. Corradini and M. Pistore. Closed interval process algebra versus interval process algebra. *Acta Informatica*, 37(7):467–509, 2001.

[11] S. Ganeriwal, R. Kumar, and M. Srivastava. Timing-Sync Protocol for Sensor Networks. In *SenSys*, pages 138–149. ACM Press, 2003.

[12] F. Ghassemi, W. Fokkink, and A. Movaghar. Restricted Broadcast Process Theory. In *SEFM*, pages 345–354. IEEE Computer Society, 2008.

[13] F. Ghassemi, W. Fokkink, and A. Movaghar. Equational Reasoning on Ad Hoc networks. In *FSEN*, To appear in Lecture Notes in Computer Science. Springer, 2009.

[14] J.C. Godskesen. A Calculus for Mobile Ad Hoc Networks. In *COORDINATION*, volume 4467 of *Lecture Notes in Computer Science*, pages 132–150. Springer Verlag, 2007.

[15] J.C. Godskesen. A Calculus for Mobile Ad-hoc Networks with Static Location Binding. To appear in the Prooceedings of EXPRESS, 2008.

[16] J.F. Groote. Specification and Verification of Real Time Systems in acp. In *PSTV*, pages 261–274. North-Holland, 1990.

[17] M. Hennessy and T. Regan. A process algebra for timed systems. *Information and Computation*, 117(2):221–239, 1995.

[18] M. Hennessy and J. Riely. A typed language for distributed mobile processes. In *Proc. 25th POPL*. ACM Press, 1998.

[19] IEEE 802.11 WG. ANSI/IEEE standard 802.11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. IEEE Computer Society, 2007.

[20] M. Kwiatkowska, G. Norman, and D. Parker. Prism: Probabilistic model checking for performance and reliability analysis. *ACM SIGMETRICS Performance Evaluation Review*, 36(4):40–45, 2009.

[21] C. Laneve and G. Zavattaro. Foundations of web transactions. In *FoSSaCS*, volume 3441 of *Lecture Notes in Computer Science*, pages 282–298. Springer, 2005.

[22] Q. Li and D. Rus. Global Clock Synchronization in Sensor Networks. *IEEE Transactions on Computers*, 55(2):214–226, 2006.

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

[24] N. Mezzetti and D. Sangiorgi. Towards a Calculus For Wireless Systems. *Electronic Notes in Theoretical Computer Science*, 158:331–353, 2006.

[25] R. Milner. *Communication and Concurrency*. Prentice Hall, 1989.

[26] R. Milner, J. Parrow, and D. Walker. A calculus of mobile processes, (Parts I and II). *Information and Computation*, 100:1–77, 1992.

[27] R. Milner and D. Sangiorgi. Barbed bisimulation. In *ICALP*, volume 623 of *Lecture Notes in Computer Science*, pages 685–695. Springer Verlag, 1992.

[28] M. Mock, R. Frings, E. Nett, and S. Trikaliotis. Continuous Clock Synchronization in Wireless Real-Time Applications. In *SRDS*, pages 125–133. IEEE Computer Society, 2000.

[29] F. Moller and C. Tofts. A Temporal Calculus of Communicating Systems. In *CONCUR*, volume 458 of *Lecture Notes in Computer Science*, pages 401–415. Springer Verlag, 1990.

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

[31] X. Nicollin and J. Sifakis. The Algebra of Timed Processes, ATP: Theory and Application. *Information and Computation*, 114(1):131–178, 1994.

[32] K.V.S. Prasad. A Calculus of Broadcasting Systems. *Science of Computer Programming*, 25(2-3), 1995.

[33] K.V.S. Prasad. Broadcasting in Time. In *COORDINATION*, volume 1061 of *Lecture Notes in Computer Science*, pages 321–338. Springer Verlag, 1996.

[34] J. Rathke, V. Sassone, and P. Sobocinski. Semantic Barbs and Biorthogonality. In *FoSSaCS*, volume 4423 of *Lecture Notes in Computer Science*, pages 302–316. Springer, 2007.

[35] G.M. Reed. A Hierarchy of Domains for Real-Time Distributed Computing. Technical Report, Oxford, 1988.

[36] M. L. Sichitiu and C. Veerarittiphan. Simple, Accurate Time Synchronization for Wireless Sensor Networks. In *WCNC*, pages 1266–1273. IEEE Computer Society, 2003.

[37] A. Singh, C. R. Ramakrishnan, and S. A. Smolka. A Process Calculus for Mobile Ad Hoc Networks. In *COORDINATION*, volume 5052 of *Lecture Notes in Computer Science*, pages 296–314, 2008.

[38] W. Su and I. Akyildiz. Time-Diffusion Synchronization Protocols for Sensor Networks. *IEEE/ACM Transactions on Networking*, 13(2):384–397, 2005.

[39] B. Sundararaman, U. Buy, and A. D. Kshemkalyani. Clock synchronization for wireless sensor networks: a survey. *Ad Hoc Networks*, 3(3):281–323, 2005.

[40] W. Yi. Real-Time Behaviour of Asynchronous Agents. In *CONCUR*, volume 458 of *Lecture Notes in Computer Science*, pages 502–520. Springer Verlag, 1990.

[41] W. Yi. *A Calculus of Real Time Systems*. Ph.D Thesis, Chalmers University, 1991.

[42] S. Yoon, C. Veerarittiphan, and M. L. Sichitiu. Tiny-sync: Tight time synchronization for wireless sensor networks. *ACM Transactions on Sensor Networks*, 3(2):81–118, 2007.

A Proofs

Proof of Theorem 3.1

By induction on the length of the proof of $M \xrightarrow{\sigma} M'$. The base cases are when the transition is derived by the application of one of the following rules:

(Time-0), (Time-t), (RcvFail), and (Zero-σ). It is straightforward to prove that the statement holds for these rules. As to the inductive case, let $M \xrightarrow{\sigma} M'$ by an application of rule (Par-σ). This implies that $M = M_1 \mid M_2$, for some M_1 and M_2, with $M_1 \xrightarrow{\sigma} M_1'$, $M_2 \xrightarrow{\sigma} M_2'$ and $M' = M_1' \mid M_2'$. As $M = M_1 \mid M_2$, the transition $M \xrightarrow{\sigma} M''$ can be derived only by applying rule (Par-σ) where $M_1 \xrightarrow{\sigma} M_1''$, $M_2 \xrightarrow{\sigma} M_2''$ and $M'' = M_1'' \mid M_2''$. By inductive hypothesis it holds that M_i' and M_i'' are syntactically the same, for $i \in \{1, 2\}$. This implies that M' and M'' are syntactically the same. □

Proof of Theorem 3.2
By induction on the structure of M. In $M = \mathbf{0}$ the statement does not apply. If M is composed by only one node and $M \xrightarrow{m!v} N$, this can be derived only by an application of rule (Snd) with $M = m[!\langle v\rangle.P]_t^\nu$ and $N = m[\langle v\rangle^{\delta_v}.P]_t^\nu$. Because sender nodes cannot perform σ-actions, there is no network M' such that $M \xrightarrow{\sigma} M'$. Let M be composed by at least two nodes. If $M \xrightarrow{m!v} N$ by an application of rule (Sync) then $M = M_1 \mid M_2$ for some M_1 and M_2, with $M_1 \xrightarrow{m!v} M_1'$, $M_2 \xrightarrow{m?v} M_2'$ and $N = M_1' \mid M_2'$ (the converse is similar). In this case the only rule for deriving a σ-transition from M is (Par-σ). However, the inductive hypothesis guarantees that $M_1 \xrightarrow{\sigma} \widehat{M}$ for no network $\widehat{M}$; then $M \xrightarrow{\sigma} M'$ for no network M'. □

In order to prove Theorem 3.3 on the Patience property, we use the following auxiliary lemmas.

Lemma A.1 *Let N be a well-formed network such that $m \notin \mathsf{nds}(N)$. Then $N \xrightarrow{m?v} N'$, for some network N'.*

Proof Let us proceed by induction on the structure of N.

- Let $N = \mathbf{0}$. By an application of rule (Zero) we have $N \xrightarrow{m?v} N$.
- Let $N = n[W]_t^\nu$, with $W ::= P \mid A$. Let us proceed by induction on the structure of W.
  - Let $W = \mathsf{nil}$. There are two cases.
    - If $m \notin \nu$ then by an application of rule (OutRng) we have $N \xrightarrow{m?v} N'$.
    - If $m \in \nu$ then by an application of rule (Exp) we have $N \xrightarrow{m?v} N'$ with $N' = n[\mathsf{nil}]_{t'}^\nu$, where $t' = \max(t, \delta_v)$.
  - Let $W = !\langle v\rangle.P$. This case is similar to the previous one.
  - $W = \sigma.P$. This case is similar to the previous one.

– $W = \langle v \rangle^r.P$. This case is similar to the previous one.

– Let $W = ?(x).P$. There are three sub-cases.

  * If $m \notin \nu$ by an application of rule (OutRng) we have $N \xrightarrow{m?v} N$.
  * If $t = 0$ and $m \in \nu$ there are two cases:
    · by an application of rules (RcvP) and (Rcv) we can derive $N \xrightarrow{m?v} N'$, with $N' = n[(x)_v.P]^{\nu}_{\delta_v}$;
    · by an application of rule (Exp) we can derive $N \xrightarrow{m?v} N'$, with $N' = n[?(x).P]^{\nu}_{\delta_v}$.
  * If $t > 0$ and $m \in \nu$ then by an application of rule (Exp) we have $N \xrightarrow{m?v} N'$, with $N' = n[?(x).P]^{\nu}_{t'}$ where $t' = \max(t, \delta_v)$.

– Let $W = \lfloor ?(x).P \rfloor Q$. This case is similar to the previous one.

– Let $W = (x)_w.P$. There are two sub-cases.

  * If $m \in \nu$ then by an application of rule (Coll), it holds that $N \xrightarrow{m?v} N' = n[(x)_{\perp}.P]^{\nu}_{t'}$ with $t' := \mathsf{max}(t,\delta_v)$.
  * If $m \notin \nu$ then by an application of rule (OutRng) we have $N \xrightarrow{m?v} N$.

– Let $W = [v = v]P_1, P_2$. By an application of rule (Then) we can apply the inductive hypothesis to conclude that the statement holds.

– Let $W = [v_1 = v_2]P_1, P_2$, with $v_1 \neq v_2$. By an application of rule (Else), this case is similar to the previous one.

– Let $W = H\langle \tilde{v} \rangle$. The constraint on guarded recursion ensures us that by an application of rule (Rec) we can apply the inductive hypothesis to conclude that the statement holds.

• Let $N = N_1 \mid N_2$. By inductive hypothesis it holds that $N_1 \xrightarrow{m?v} N_1'$ and $N_2 \xrightarrow{m?v} N_2'$, for some N_1', N_2'. By an application of rule (RcvPar) it holds that $N \xrightarrow{m?v} N'$, for $N' = N_1' \mid N_2'$.

□

Lemma A.2 *Let M be a well-formed network. If $M \xrightarrow{m!v} M'$ then for all network N such that $M \mid N$ is a well-formed network it holds that $M \mid N \xrightarrow{m!v} M' \mid N'$ for some network N'.*

Proof The result follows by Lemma A.1 and an application of rule (Sync).

□

Proof of Theorem 3.3
By contradiction and then by induction on the structure of M. We prove that if $M \xrightarrow{\sigma} N$ for no network N then $M \xrightarrow{m!v} M'$ for some network M'. Let us proceed by induction on the structure of M.

- Let $M = \mathbf{0}$. Then $M \xrightarrow{\sigma} M$ by an application of rule (Zero-σ). So, the statement does not apply.
- Let $M = n[W]^{\nu}_{t}$. We proceed by induction on the structure of P.
  - If $W = \mathsf{nil}$ and $t = 0$ then $M \xrightarrow{\sigma} n[P]^{\nu}_{0}$ by an application of rules (Nil-σ and) and (Time-0). Thus the statement does not apply.
  - If $W = \mathsf{nil}$ and $t > 0$ then $M \xrightarrow{\sigma} n[P]^{\nu}_{t-1}$ by an application of rules (Nil-σ and) and (Time-t). Thus the statement does not apply.
  - If $W = !\langle v\rangle.P$ then $M \not\xrightarrow{\sigma}$. However, $M \xrightarrow{m!v} m[\langle v\rangle^{\delta_v}.P]^{\nu}_{t}$, by an application of rule (Snd), in contradiction with the hypothesis.
  - If $W = ?(x).P$ and $t = 0$ then $M \xrightarrow{\sigma} n[W]^{\nu}_{0}$, by an application of rules (Rcv-σ) and (Time-0). Thus the statement does not apply.
  - If $W = ?(x).P$ and $t = 1$ then $M \xrightarrow{\sigma} n[\{^{\perp}/_{x}\}P]^{\nu}_{0}$, by an application of rules (RcvP) and (RcvFail). Thus the statement does not apply.
  - If $W = ?(x).P$ and $t > 1$ then $M \xrightarrow{\sigma} n[(x)_{\perp}.P]^{\nu}_{t-1}$, by an application of rules (RcvP) and (RcvFail). Thus the statement does not apply.
  - If $W = \sigma.P$ and $t = 0$ then $M \xrightarrow{\sigma} n[W]^{\nu}_{0}$ by an application of rules (Sigma) and (Time-0). Thus the statement does not apply.
  - If $W = \sigma.P$ and $t > 0$ then $M \xrightarrow{\sigma} n[W]^{\nu}_{t-1}$ by an application of rules (Sigma) and (Time-t). Thus the statement does not apply.
  - If $W = \lfloor ?(x).P \rfloor Q$ and $t = 0$ then $M \xrightarrow{\sigma} n[Q]^{\nu}_{t\ominus 1}$, by an application of rules (Timeout) and (Time-0). Thus the statement does not apply.
  - If $W = \lfloor ?(x).P \rfloor Q$ and $t = 1$ then $M \xrightarrow{\sigma} n[\{^{\perp}/_{x}\}P]^{\nu}_{0}$, by an application of rules (RcvP) and (RcvFail). and the statement does not apply.
  - If $W = \lfloor ?(x).P \rfloor Q$ and $t > 1$ then $M \xrightarrow{\sigma} n[(x)_{\perp}.P]^{\nu}_{t-1}$, by an application of rules (RcvP) and (RcvFail), Thus the statement does not apply.
  - If $W = [v = v]P_1, P_2$ then by an application of rule (Then) we can apply the inductive hypothesis to conclude that we fall in one of the previous cases.

- If $W = [v_1 = v_2]P_1, P_2$, with $v_1 \neq v_2$, by an application of rule (Else) we can apply the inductive hypothesis to conclude that we fall in one of the previous cases.
- If $W = H\langle\tilde{v}\rangle$ the constraint of guarded recursion ensures us that by an application of rule (Rec) we can apply the inductive hypothesis and we fall in one of the previous cases.
- If $W = \langle v\rangle^r.P$, with $r > 1$, and $t = 0$ then by an application of rules (ActSnd) and (Time-0) we have $M \xrightarrow{\sigma} n[\langle v\rangle^{r-1}.P]_0^\nu$ and the statement does not apply.
- If $W = \langle v\rangle^r.P$, with $r > 1$, and $t > 0$ then by an application of rules (ActSnd) and (Time-t) we have $M \xrightarrow{\sigma} n[\langle v\rangle^{r-1}.P]_{t-1}^\nu$ and the statement does not apply.
- If $W = \langle v\rangle.P$ and $t = 0$, then by an application of rules (ActSnd) and (Time-0) we have $M \xrightarrow{\sigma} n[P]_0^\nu$ and the statement does not apply.
- If $W = \langle v\rangle.P$ and $t > 0$, then by an application of rules (ActSnd) and (Time-t) we have $M \xrightarrow{\sigma} n[P]_{t-1}^\nu$ and the statement does not apply.
- If $W = (x)_v.P$, with $t > 0$, then by an application of rules (ActRcv) and (Time-t) we have $M \xrightarrow{\sigma} n[(x)_v.P]_{t\ominus 1}^\nu$ and the statement does not apply.
- If $W = (x)_v.P$, with $t = 0$, then by an application of rules (ActRcv) and (Time-0) we have $M \xrightarrow{\sigma} n[\{^v/_x\}P]_0^\nu$ and the statement does not apply.

- Let $M = M_1 \mid M_2$. A transition of the form $M \xrightarrow{\sigma} M'$ can be derived only by an application of rule (Par-σ). Thus if M cannot perform a σ-action then at least one of the premises of rule (Par-σ) does not hold:
  - If $M_1 \xrightarrow{\sigma} M_1'$ for no network M_1', then by inductive hypothesis we have $M_1 \xrightarrow{m!v} M_1'$, for some M_1'. As $M = M_1 \mid M_2$ is a well-formed network, by Lemma A.2 it holds that $M \xrightarrow{m!v} M_1' \mid M_2'$, for some M_2', in contradiction with the hypothesis.
  - If $M_2 \xrightarrow{\sigma} M_2'$ for no network M_2', then we can reason as in the previous sub-case.

□

Now, we prove that our operational semantics preserves network well-formedness.

Proposition A.3 *Let M be a node-unique network. If $M \xrightarrow{\lambda} M'$ then M' is node-unique.*

Proof By transition induction. □

Proposition A.4 *Let M be a connected network. If $M \xrightarrow{\lambda} M'$ then M' is connected.*

Proof By transition induction. Notice that no inference rule changes the network topology. □

Now, let us prove that our LTS preserves exposure consistency. For that we need the two following technical lemmas.

Lemma A.5 *Let $M \xrightarrow{\lambda} M'$ with $\lambda \in \{m!v, m?v\}$ such that $M \equiv \prod_{i\in} n_i[W_i]^{\nu_i}_{t_i}$ and $M' \equiv \prod_{i\in I} n_i[W'_i]^{\nu_i}_{t'_i}$.*

1. *If $\lambda = m?v$ then $m \neq n_i$, for all i.*
2. *If $\lambda = m!v$ then there is $i \in I$ such that $m = n_i$, $W_i = !\langle v\rangle.P_i$ and $W'_i = \langle v\rangle^{\delta_v}.P_i$.*
3. *If $m \notin \nu_i$, for some i, then $t'_i = t_i$; if also $m \neq n_i$, then $W'_i = W_i$.*
4. *If $m \in \nu_i$, for some i, then $t'_i = \max(t_i, \delta_v)$.*
5. *If $m \in \nu_i$ and $W'_i{=}(x)_w.P_i$, for some i, and $w{\neq}\bot$, then $w = m{:}v$, $t_i = 0$, $t'_i = \delta_v$, and $W_i \ ::= \ ?(x).P_i \ \mid \ \lfloor ?(x).P_i \rfloor Q_i$,*
6. *If $W_i = \langle w\rangle^r.P_i$, for some i, then $W'_i = W_i$.*
7. *If $m \neq n_i$ and $W'_i = \langle w\rangle^r.P_i$, for some i, then $W_i = W'_i$.*

Proof By transition induction. □

Lemma A.6 *Let $M \xrightarrow{\sigma} M'$ such that $M \equiv \prod_{i\in} n_i[W_i]^{\nu_i}_{t_i}$ and $M' \equiv \prod_{i\in I} n_i[W'_i]^{\nu_i}_{t'_i}$.*

1. *$t'_i = t_i \ominus 1$, for all i.*
2. *If $W'_i = (x)_v.P$, for some i, then*
   - *either $W_i = W'_i$*
   - *or $W_i \ ::= ?(x).P \ \mid \ \lfloor ?(x).P \rfloor Q$ and $v = \bot$*
3. *If $W'_i = \langle w\rangle^r.P$, for some i, then $W_i = \langle w\rangle^{r+1}.P$.*

Proof By transition induction. □

We can prove now the preservation of exposure consistency.

Proposition A.7 (Exposure consistency) *Let M be an exposure consistent network. If $M \xrightarrow{\lambda} M'$ then M' is exposure consistent.*

Proof The proof proceeds by transition induction on the derivation of $M \xrightarrow{\lambda} M'$, for $\lambda \in \{m!v, m?v, \sigma\}$. We show the most significant cases, derived by an application of rules (Sync), (RcvPar), and (Par-σ). The other cases are straightforward.

- Let $M \xrightarrow{m!v} M'$ by an application of rule (Sync) with $M = M_1 \mid M_2$, $M_1 \xrightarrow{m!v} M_1'$ and $M_2 \xrightarrow{m?v} M_2'$, and $M' = M_1' \mid M_2'$, where M_1' and M_2' are exposure consistent by inductive hypothesis. We have to prove that M' respects the clauses of Definition 2.5.
  - Clauses 1-2. In these cases the result follows directly by inductive hypothesis.
  - Clause 3. Let $M' \equiv \prod_i n_i[W_i']_{t_i'}^{\nu_i} \mid h[\langle v\rangle^r.P]_{t_h'}^{\nu_h} \mid n[W']_{t_n'}^{\nu_n}$, with $h \in \nu_n$. We have to prove that $r \leq t_n'$. We only consider the case when $h \in \mathsf{nds}(M_1)$ and $n \in \mathsf{nds}(M_2)$ (or viceversa). The other cases are easier. There are two possibilities.
    - $h \neq m$. By Lemma A.5(7) we have
    $$M \equiv \prod_i n_i[W_i]_{t_i}^{\nu_i} \mid h[\langle v\rangle^r.P]_{t_h}^{\nu_h} \mid n[W]_{t_n}^{\nu_n}$$
    for appropriate processes and tags. Now, if $m \in \nu_n$ by Lemma A.5(4) we have $t_n' = \max(t_n, \delta_v)$. As M is exposure consistent it holds that $r \leq t_n$ and hence also $r \leq t_n'$. On the other hand, if $m \notin \nu_n$ by an application of Lemma A.5(3) we have $t_n' = t_n$. As M is exposure consistent it follows that $r \leq t_n = t_n'$.
    - $h = m$. By Lemma A.5(2) it follows that
    $$M \equiv \prod_i n_i[W_i]_{t_i}^{\nu_i} \mid h[!\langle v\rangle.P]_{t_h}^{\nu_h} \mid n[W]_{t_n}^{\nu_n}$$
    for appropriate processes and tags, with $r = \delta_v$. Since $h \in \nu_n$, by Lemma A.5(4) we have $t_n' = \max(t_n, \delta_v)$. As a consequence, $r \leq t_n'$.
  - Clause 4. Let
  $$M \equiv N \mid n[W]_t^{\nu} = \prod_i n_i[W_i]_{t_i}^{\nu_i} \mid n[W]_t^{\nu}$$

and

$$M' \equiv N' \mid n[W']^{\nu}_{t'} = \prod_i n_i[W'_i]^{\nu_i}_{t'_i} \mid n[W']^{\nu}_{t'}$$

with $t' > 0$ and $\mathsf{active}(k', N') \neq t'$ for all $k' \in \nu \cap \mathsf{actsnd}(N')$. We have to prove that there is $\hat{k} \in \nu \setminus \mathsf{nds}(N')$ such that if $\hat{k} \in \nu_i$, for some i, then $t'_i \geq t'$. We can distinguish two cases:

* If $m \notin \nu$ by Lemma A.5(3) we have $t' = t$. By Lemma A.5(6), it follows that $\mathsf{actsnd}(N) \subseteq \mathsf{actsnd}(N')$. As a consequence, $\nu \cap \mathsf{actsnd}(N) \subseteq \nu \cap \mathsf{actsnd}(N')$. Since $t' = t$ we can derive that for all $k \in \nu \cap \mathsf{actsnd}(N)$ it holds that $\mathsf{active}(k, N') \neq t$. By Lemma A.5(6) and Lemma A.5(7) if $k \neq m$ then $\mathsf{active}(k, N) = \mathsf{active}(k, N')$. Since $m \notin \nu$ it follows that for all $k \in \nu \cap \mathsf{actsnd}(N)$ it holds $\mathsf{active}(k, N) \neq t$. Since M is exposure consistent it follows that there is $\hat{k} \in \nu \setminus \mathsf{nds}(N)$ such that if $\hat{k} \in \nu_i$, for some i, then $t_i \geq t$. Notice that $\nu \setminus \mathsf{nds}(N) = \nu \setminus \mathsf{nds}(N')$. Moreover, by Lemma A.5(3) and A.5(4) we have $t_i \leq t'_i$, for all i. This allows us to derive that there is $\hat{k} \in \nu \setminus \mathsf{nds}(N')$ such that if $\hat{k} \in \nu_i$, for some i, then $t'_i \geq t_i \geq t = t'$.
* If $m \in \nu$ then by Lemma A.5(4) we have $t' = \max(t, \delta_v)$. By definition of neighbouring of a node $m \in \nu$ implies $m \neq n$. By Lemma A.5(2) it follows that $m \notin \mathsf{actsnd}(N)$, $m \in \mathsf{actsnd}(N')$, and $\mathsf{active}(m, N') = \delta_v$. Since $\mathsf{active}(k', N') \neq t'$ for all $k' \in \nu \cap \mathsf{actsnd}(N')$, and $m \in \nu \cap \mathsf{actsnd}(N')$, it follows that $t' \neq \delta_v$. Since $t' = \max(t, \delta_v)$, it follows that $t' = t$. By Lemma A.5(6), it follows that $\mathsf{actsnd}(N) \subseteq \mathsf{actsnd}(N')$. As a consequence, $\nu \cap \mathsf{actsnd}(N) \subseteq \nu \cap \mathsf{actsnd}(N')$. Since $t' = t$ we can derive that for all $k \in \nu \cap \mathsf{actsnd}(N)$ it holds that $\mathsf{active}(k, N') \neq t$. By Lemma A.5(6) and Lemma A.5(7) if $k \neq m$ then $\mathsf{active}(k, N) = \mathsf{active}(k, N')$. Since $m \notin \mathsf{actsnd}(N)$ it follows that for all $k \in \nu \cap \mathsf{actsnd}(N)$ it holds $\mathsf{active}(k, N) \neq t$. Since M is exposure consistent it follows that there is $\hat{k} \in \nu \setminus \mathsf{nds}(N)$ such that if $\hat{k} \in \nu_i$, for some i, then $t_i \geq t$. Notice that $\nu \setminus \mathsf{nds}(N) = \nu \setminus \mathsf{nds}(N')$. Moreover, by Lemmas A.5(3) and A.5(4) we have $t_i \leq t'_i$, for all i. This allows us to derive that there is $\hat{k} \in \nu \setminus \mathsf{nds}(N')$ such that if $\hat{k} \in \nu_i$, for some i, then $t'_i \geq t_i \geq t = t'$.

- Let $M \xrightarrow{m?v} M'$ by an application of rule (RcvPar) with $M = M_1 \mid M_2$, $M_1 \xrightarrow{m?v} M'_1$, $M_2 \xrightarrow{m?v} M'_2$, and $M' = M'_1 \mid M'_2$, where both M'_1 and M'_2 are exposure consistent by inductive hypothesis. We have to prove that M' respects the clauses of Definition 2.5.

– Clauses 1-2. We reason as in the case of the the sending action $m!v$ examined above.

– Clause 3. Let $M' \equiv \prod_i n_i[W_i']^{\nu_i}_{t_i'} \mid h[\langle v\rangle^r.P]^{\nu_h}_{t_h'} \mid n[W']^{\nu_n}_{t_n'}$, with $h \in \nu_n$. We have to prove that $r \leq t_n'$. We only consider the case when $h \in \mathsf{nds}(M_1)$ and $n \in \mathsf{nds}(M_2)$ (or viceversa). The other cases are easier. By Lemma A.5(1) it holds that $m \notin \mathsf{nds}(M')$. By A.5(7) it follows:

$$M \equiv \prod_i n_i[W_i]^{\nu_i}_{t_i} \mid h[\langle v\rangle^r.P]^{\nu_h}_{t_h} \mid n[W]^{\nu_n}_{t_n}$$

for appropriate processes and tags. Now, if $m \in \nu_n$ by Lemma A.5(4) we have $t_n' = \max(t_n, \delta_v)$. As M is exposure consistent it holds that $r \leq t_n$ and hence also $r \leq t_n'$. On the other hand, if $m \notin \nu_n$ by an application of Lemma A.5(3) we have $t_n' = t_n$; as M is exposure consistent it follows that $r \leq t_n = t_n'$.

– Clause 4. Let

$$M \equiv N \mid n[W]^{\nu}_{t} = \prod_i n_i[W_i]^{\nu_i}_{t_i} \mid n[W]^{\nu}_{t}$$

and

$$M' \equiv N' \mid n[W']^{\nu}_{t'} = \prod_i n_i[W_i']^{\nu_i}_{t_i'} \mid n[W']^{\nu}_{t'}$$

with $t' > 0$ and $\mathsf{active}(k', N') \neq t'$ for all $k' \in \nu \cap \mathsf{actsnd}(N')$. We have to prove that there is $\hat{k} \in \nu \setminus \mathsf{nds}(N')$ such that if $\hat{k} \in \nu_i$, for some i, then $t_i' \geq t'$. There are two cases.

* Let $m \notin \nu$. By Lemma A.5(3) we have $t' = t$. By Lemma A.5(6), it follows that $\mathsf{actsnd}(N) \subseteq \mathsf{actsnd}(N')$. As a consequence, $\nu \cap \mathsf{actsnd}(N) \subseteq \nu \cap \mathsf{actsnd}(N')$. Since $t' = t$ we can derive that for all $k \in \nu \cap \mathsf{actsnd}(N)$ it holds that $\mathsf{active}(k, N') \neq t$. By Lemma A.5(6) and Lemma A.5(7) if $k \neq m$ then $\mathsf{active}(k, N) = \mathsf{active}(k, N')$. Since $m \notin \nu$ it follows that for all $k \in \nu \cap \mathsf{actsnd}(N)$ it holds $\mathsf{active}(k, N) \neq t$. Since M is exposure consistent it follows that there is $\hat{k} \in \nu \setminus \mathsf{nds}(N)$ such that if $\hat{k} \in \nu_i$, for some i, then $t_i \geq t$. Notice that $\nu \setminus \mathsf{nds}(N) = \nu \setminus \mathsf{nds}(N')$. Moreover, by Lemma A.5(3) and A.5(4) we have $t_i \leq t_i'$, for all i. This allows us to derive that there is $\hat{k} \in \nu \setminus \mathsf{nds}(N')$ such that if $\hat{k} \in \nu_i$, for some i, then $t_i' \geq t_i \geq t = t'$.
* Let $m \in \nu$. By Lemma A.5(1) we have $m \notin \mathsf{nds}(M)$. By Lemmas A.5(6) and A.5(7) for all $k \in \mathsf{nds}(N)$ it holds that $\mathsf{active}(k, N) =$

$\mathsf{active}(K, N')$. As a consequence, $\mathsf{actsnd}(N) = \mathsf{actsnd}(N')$, and hence $\nu \cap \mathsf{actsnd}(N) = \nu \cap \mathsf{actsnd}(N')$. By Lemma A.5(4) we have $t' = \max(t, \delta_v)$. So, there are two cases.

- Let $\delta_v \leq t$. Then $t' = t$ and for all $k \in \nu \cap \mathsf{actsnd}(N)$ it holds $\mathsf{active}(k, N) \neq t$. Since M is exposure consistent it follows that there is $\hat{k} \in \nu \setminus \mathsf{nds}(N)$ such that if $\hat{k} \in \nu_i$, for some i, then $t_i \geq t$. Notice that $\nu \setminus \mathsf{nds}(N) = \nu \setminus \mathsf{nds}(N')$. Moreover, by Lemmas A.5(3) and A.5(4) we have $t_i \leq t'_i$, for all i. This allows us to derive that there is $\hat{k} \in \nu \setminus \mathsf{nds}(N')$ such that if $\hat{k} \in \nu_i$, for some i, then $t'_i \geq t_i \geq t = t'$.
- Let $\delta_v > t$. Then $t' = \delta_v$. In this case, there is $m \in \nu \setminus \mathsf{nds}(N')$ such that if $m \in \nu_i$, for some i, then by Lemma A.5(4) it holds that $t'_i = \max(t_i, \delta_v)$. Thus, $t'_i \geq \delta_v = t'$.

- Let $M \xrightarrow{\sigma} M'$ by an application of rule (Par-σ) with $M = M_1 \mid M_2$, $M_1 \xrightarrow{\sigma} M'_1$ and $M_2 \xrightarrow{\sigma} M'_2$, and $M' = M'_1 \mid M'_2$, where both M'_1 and M'_2 are exposure consistent by inductive hypothesis. We have to prove that M' respects the clauses of Definition 2.5.

  - Clauses 1-2. It is easy to show that M' is exposure consistent. The results follow by inductive hypothesis.
  - Clause 3. Let

    $$M' \equiv \prod_i n_i[W'_i]^{\nu_i}_{t'_i} \mid h[\langle v \rangle^r.P]^{\nu_h}_{t'_h} \mid n[W']^{\nu_n}_{t'_n}$$

    with $h \in \nu_n$. We have to prove that $r \leq t'_n$. We only consider the case when $h \in \mathsf{nds}(M_1)$ and $n \in \mathsf{nds}(M_2)$ (or viceversa). The other cases are easier. By Lemma A.6(1) and A.6(3) we have

    $$M \equiv \prod_i n_i[W_i]^{\nu_i}_{t_i} \mid h[\langle v \rangle^{r+1}.P]^{\nu_h}_{t_h} \mid n[W]^{\nu_n}_{t'_n+1}$$

    for appropriate processes and tags. As M is exposure consistent, it follows that $r \leq t'_n$.
  - Clause 4. Let

    $$M \equiv N \mid n[W]^{\nu}_{t} = \prod_i n_i[W_i]^{\nu_i}_{t_i} \mid n[W]^{\nu}_{t}$$

    and

    $$M' \equiv N' \mid n[W']^{\nu}_{t'} = \prod_i n_i[W'_i]^{\nu_i}_{t'_i} \mid n[W']^{\nu}_{t'}$$

with $t' > 0$ and $\mathsf{active}(k', N') \neq t'$ for all $k' \in \nu \cap \mathsf{actsnd}(N')$. We have to prove that there is $\hat{k} \in \nu \setminus \mathsf{nds}(N')$ such that if $\hat{k} \in \nu_i$, for some i, then $t'_i \geq t'$. By Lemma A.6(1) we have $t' = t \ominus 1$. Since $t' > 0$ it follows that $t > 1$. Moreover, by Lemma A.6(3), if $W'_i = \langle w \rangle^{r'}.Q$, for some i, then $W_i = \langle w \rangle^{r}.Q$, with $r' = r \ominus 1$. As a consequence, $\mathsf{actsnd}(N') \subseteq \mathsf{actsnd}(N)$. By Lemma A.6(3) if $\mathsf{active}(k', N') \neq t'$ then $\mathsf{active}(k', N) \neq t' + 1 = t$. Notice also that $\mathsf{active}(k, N) = 1$ for all $k \in \mathsf{actsnd}(N) \setminus \mathsf{actsnd}(N')$. Thus, since $t > 1$ for all $k \in \nu \cap \mathsf{actsnd}(N)$ it holds that $\mathsf{active}(k, N) \neq t$. Since M is exposure consistent it follows that there is $\hat{k} \in \nu \setminus \mathsf{nds}(N)$ such that if $\hat{k} \in \nu_i$, for some i, then $t_i \geq t$. Notice that $\nu \setminus \mathsf{nds}(M) = \nu \setminus \mathsf{nds}(M')$. Moreover, by Lemma A.6(1) we have $t'_i = t_i \ominus 1$, for all i. This allows us to derive that there is $\hat{k} \in \nu \setminus \mathsf{nds}(N')$ such that if $\hat{k} \in \nu_i$, for some i, then $t'_i \geq t'$.

□

Let us prove now that our LTS preserves transmission consistency.

Proposition A.8 (Transmission consistency) *Let M be both an exposure consistent and a transmission consistent network. If $M \xrightarrow{\lambda} M'$ then M' is transmission consistent.*

Proof Let us consider all the possible values of λ.

- Let $M \xrightarrow{m!v} M'$. We have to prove that M' respects the clauses of Definition 2.6. Let examine the three clauses one by one.
  - Clause 1. Let

$$M' \equiv N' \mid n[(x)_w.Q]^{\nu_n}_{t'_n} = \prod_i n_i[W'_i]^{\nu_i}_{t'_i} \mid n[(x)_w.Q]^{\nu_n}_{t'_n}$$

    with $w \neq \bot$. We have to prove that $\mid \mathsf{actsnd}(N') \cap \nu \mid \leq 1$. By Lemma A.5(2) we have

$$M' \equiv N' \mid n[(x)_w.Q]^{\nu_n}_{t'_n} \equiv \prod_j n_j[W'_j]^{\nu_j}_{t'_j} \mid m[\langle v \rangle^{\delta_v}.P]^{\nu_m}_{t'_m} \mid n[(x)_w.Q]^{\nu_n}_{t'_n}$$

    and

$$M \equiv N \mid n[W]^{\nu_n}_{t'_n} = \prod_j n_j[W_j]^{\nu_j}_{t_j} \mid m[!\langle v \rangle.P]^{\nu_m}_{t_m} \mid n[W]^{\nu_n}_{t_n}$$

    for appropriate processes and tags.

    There are two possibilities.

* If $m \notin \nu_n$ then by Lemma A.5(3) we have $W = (x)_w.Q$. By Lemmas A.5(6) and A.5(7) we have $\mathsf{actsnd}(N') = \mathsf{actsnd}(N) \cup \{m\}$. Since M is transmission consistent, we have $\mid \mathsf{actsnd}(N) \cap \nu_n \mid \leq 1$. Since $m \notin \nu_n$ it follows that $\mid \mathsf{actsnd}(N') \cap \nu_n \mid \leq 1$.
* If $m \in \nu$ then by Lemma A.5(5) we have $W = ?(x).Q$ (the case $W = \lfloor ?(x).P \rfloor Q$ is similar) and $t_n = 0$. By Lemmas A.5(6) and A.5(7) we have $\mathsf{actsnd}(N') = \mathsf{actsnd}(N) \cup \{m\}$. Since $t_n = 0$, $m \in \nu_n$, and M is exposure consistent, clause 3 of Definition 2.5 allows to derive that $\mathsf{actsnd}(N') \cap \nu_n = \{m\}$. Hence, $\mid \mathsf{actsnd}(N') \cap \nu_n \mid \leq 1$.

– Clause 2. Let

$$M' \equiv \prod_i n_i[W_i']_{t_i'}^{\nu_i} \mid h[\langle w_1 \rangle^r.P]_{t_h'}^{\nu_h} \mid n[(x)_{w_2}.Q]_{t_n'}^{\nu_n}$$

with $h \in \nu_n$ and $w_2 \neq \bot$. We have to show that $w_2 = m{:}w_1$ and $r = t_n'$. There are two cases.

1. Suppose $h \neq m$. In this case, by Lemma A.5(2) we have the following situation:

$$M' \equiv \prod_j n_j[W_j']_{t_j'}^{\nu_j} \mid m[\langle v \rangle^{\delta_v}.R]_{t_m'}^{\nu_m} \mid h[\langle w_1 \rangle^r.P]_{t_h'}^{\nu_h} \mid n[(x)_{w_2}.Q]_{t_n'}^{\nu_n}$$

and

$$M \equiv \prod_j n_j[W_j]_{t_j}^{\nu_j} \mid m[!\langle v \rangle.R]_{t_m}^{\nu_m} \mid h[\langle w_1 \rangle^r.P]_{t_h}^{\nu_h} \mid n[W]_{t_n}^{\nu_n}$$

for appropriate processes and tags.
Now, there are two sub-cases.
   (a) If $m \notin \nu_n$ then by Lemma A.5(3) we have $W = (x)_{w_2}.Q$ and $t_n' = t_n$. Since M is transmission consistent we derive $w_2 = m{:}w_1$ and $r = t_n'$.
   (b) If $m \in \nu_n$ then by Lemma A.5(5) we have $W = ?(x).Q$ (the case $W = \lfloor ?(x).P \rfloor Q$ is similar) and $t_n = 0$. However, since M is exposure consistent by clause 3 of Definition 2.5 it must be $t_n > 0$. So, this case is not possible.
2. Suppose $h = m$. This case easily follows by an application of Lemma A.5(2) and Lemma A.5(5).

– Clause 3. Let

$$M' \equiv N' \mid n[(x)_w.P]^{\nu_n}_{t'_n} = \prod_i n_i[W'_i]^{\nu_i}_{t'_i} \mid n[(x)_w.P]^{\nu_n}_{t'_n}$$

with $\mid \mathsf{actsnd}(N') \cap \nu_n \mid > 1$. We want to show that $w = \bot$. By an application of Lemma A.5(2) it holds that

$$M' \equiv \prod_j n_j[W'_j]^{\nu_j}_{t'_j} \mid m[\langle v \rangle^{\delta v}.Q]^{\nu_m}_{t'_m} \mid n[(x)_w.P]^{\nu_n}_{t'_n}$$

and

$$M \equiv \prod_j n_j[W_j]^{\nu_j}_{t_j} \mid m[!\langle v \rangle.Q]^{\nu_m}_{t_m} \mid n[W]^{\nu_n}_{t_n}$$

for appropriate processes and tags. Since $\mid \mathsf{actsnd}(N') \cap \nu_n \mid > 1$, it must be $W'_j = \langle w_j \rangle^r.P_j$, for some j. By Lemma A.5(6) we derive that $W_j = W'_j$. At this point we reason by contradiction. Suppose $w \neq \bot$. Then, by Lemma A.5(5) we have $W = ?(x).P$ (the case $W = \lfloor ?(x).P \rfloor Q$ is similar) and $t_n = 0$. However, since M is exposure consistent, by clause 3 of Definition 2.5 it must be $t_n > 0$. This contradiction allows us to conclude that $w = \bot$.

- Let $M \xrightarrow{m?v} M'$. We have to prove that M' respect the clauses of Definition 2.6.

  – Clause 1. Let

  $$M' \equiv N' \mid n[(x)_w.Q]^{\nu_n}_{t'_n} = \prod_i n_i[W'_i]^{\nu_i}_{t'_i} \mid n[(x)_w.Q]^{\nu_n}_{t'_n}$$

  with $w \neq \bot$. We have to prove that $\mid \mathsf{actsnd}(N') \cap \nu_n \mid \leq 1$. There are two possibilities.

  * If $m \notin \nu_n$ then by Lemma A.5(3) we have

  $$M \equiv N \mid n[(x)_w.Q]^{\nu_n}_{t_n} = \prod_i n_i[W_i]^{\nu_i}_{t_i} \mid n[(x)_w.Q]^{\nu_n}_{t_n} \ .$$

  Since M is transmission consistent, we have $\mid \mathsf{actsnd}(N) \cap \nu_n \mid \leq 1$. By Lemmas A.5(6) and A.5(7) we derive $\mathsf{actsnd}(N') = \mathsf{actsnd}(N)$. This allows us to derive that $\mid \mathsf{actsnd}(N') \cap \nu_n \mid \leq 1$.
  * If $m \in \nu_n$, since $w \neq \bot$, by Lemma A.5(5) we have

  $$M \equiv N \mid n[W]^{\nu_n}_0 = \prod_i n_i[W_i]^{\nu_i}_{t_i} \mid n[?(x).Q]^{\nu_n}_0$$

where $t'_n = \delta_v$ and $W = ?(x).Q$ (the case $W = \lfloor ?(x).Q \rfloor R$ is similar). By Lemmas A.5(6) and A.5(7) we derive $\mathsf{actsnd}(N') = \mathsf{actsnd}(N)$. Since M is exposure consistent, by clause 3 of Definition 2.5 we derive $\mid \mathsf{actsnd}(N) \cap \nu_n \mid = 0$. As a consequence, $\mid \mathsf{actsnd}(N') \cap \nu_n \mid = 0$.

– Clause 2. Let

$$M' \equiv \prod_i n_i[W'_i]^{\nu_i}_{t'_i} \mid h[\langle w_1 \rangle^r.P]^{\nu_h}_{t'_h} \mid n[(x)_{w_2}.Q]^{\nu_n}_{t'_n}$$

with $h \in \nu_n$ and $w_2 \neq \bot$. We have to show that $w_2 = m{:}w_1$ and $r = t'_n$. By Lemma A.5(1) we have $h \neq m$. By Lemmas A.5(7) we have

$$M \equiv \prod_i n_i[W_i]^{\nu_i}_{t_i} \mid h[\langle w_1 \rangle^r.P]^{\nu_h}_{t_h} \mid n[W]^{\nu_n}_{t_n}$$

for appropriate processes and tags. Now, there are two cases.

* If $m \notin \nu_n$ then by Lemma A.5(3) we have $W = (x)_{w_2}.Q$ and $t'_n = t_n$. Since M is transmission consistent it follows that $w_2 = m : w_1$ and $t'_n = r$.
* If $m \in \nu_n$ then by Lemma A.5(5) we have $W = ?(x).Q$ (the case $W = \lfloor ?(x).P \rfloor Q$ is similar) and $t_n = 0$. Since M is exposure consistent, by clause 3 of Definition 2.5 it should be $t_n > 0$. This contradiction shows that this case is not possible.

– Clause 3. Let

$$M' \equiv N' \mid n[(x)_w.P]^{\nu_n}_{t'_n} = \prod_i n_i[W'_i]^{\nu_i}_{t'_i} \mid n[(x)_w.P]^{\nu_n}_{t'_n}$$

with $\mid \mathsf{actsnd}(N') \cap \nu_n \mid > 1$. We have to show that $w = \bot$. By Lemma A.5 we have

$$M \equiv \prod_i n_i[W_i]^{\nu_i}_{t_i} \mid n[W]^{\nu_n}_{t_n}$$

for appropriate processes and tags. Since $\mid \mathsf{actsnd}(N') \cap \nu_n \mid > 1$ it follows that $W'_j = \langle w_j \rangle^{r_j}.P_j$ and $W'_k = \langle w_k \rangle^{r_k}.P_k$, for some j and k such that $\{n_j, n_k\} \subseteq \nu_n$. By Lemma A.5(1) and Lemma A.5(7) we have $W_j = W'_j$ and $W_k = W'_k$. At this point we reason by contradiction. Suppose $w \neq \bot$. Then, by Lemma A.5(5) we have $W = ?(x).P$ (the case $W = \lfloor ?(x).P \rfloor Q$ is similar) and $t_n = 0$. However, since M is exposure consistent, by clause 3 of Definition 2.5 it must be $t_n > 0$. This contradiction allows us to derive that $w = \bot$.

- Let $M \xrightarrow{\sigma} M'$. We have to prove that M' respects the clauses of Definition 2.6. Let us examine the three clauses one by one.
  - Clause 1. Let
    $$M' \equiv N' \mid n[(x)_w.Q]^{\nu_n}_{t'_n} = \prod_i n_i[W'_i]^{\nu_i}_{t'_i} \mid n[(x)_w.Q]^{\nu_n}_{t'_n}$$
    with $w \neq \bot$. We have to prove that $\mid \mathsf{actsnd}(N') \cap \nu_n \mid \leq 1$. By Lemma A.6(2), since $w \neq \bot$, it must bu
    $$M \equiv N \mid n[(x)_w.Q]^{\nu_n}_{t_n} = \prod_i n_i[W_i]^{\nu_i}_{t_i} \mid n[(x)_w.Q]^{\nu_n}_{t_n}$$
    Since M is transmission consistent it follows that $\mid \mathsf{actsnd}(N) \cap \nu \mid \leq 1$. By Lemma A.6(3) it follows that $\mathsf{actsnd}(N') \subseteq \mathsf{actsnd}(N)$. This implies $\mid \mathsf{actsnd}(N') \cap \nu \mid \leq 1$.
  - Clause 2. Let
    $$M' \equiv \prod_i n_i[W'_i]^{\nu_i}_{t'_i} \mid h[\langle w_1 \rangle^r.P]^{\nu_h}_{t'_h} \mid n[(x)_{w_2}.Q]^{\nu_n}_{t'_n}$$
    with $h \in \nu_n$ and $w_2 \neq \bot$. We have to show that $w_2 = m{:}w_1$ and $r = t'_n$. Since $w_2 \neq \bot$, by Lemmas A.6(1), A.6(2), and A.6(3)
    $$M \equiv \prod_i n_i[W_i]^{\nu_i}_{t_i} \mid h[\langle w_1 \rangle^{r+1}.P]^{\nu_h}_{t_h} \mid n[(x)_{w_2}.Q]^{\nu_n}_{t'_n+1} \ .$$
    Since M is transmission consistent we have $w_2 = m{:}w_1$ and $r + 1 = t'_n + 1$. As a consequence, $r = t'_n$.
  - Clause 3. Let
    $$M' \equiv N' \mid n[(x)_w.P]^{\nu_n}_{t'_n} = \prod_i n_i[W'_i]^{\nu_i}_{t'_i} \mid n[(x)_w.P]^{\nu_n}_{t'_n}$$
    with $\mid \mathsf{actsnd}(N') \cap \nu_n \mid > 1$. We have to show that $w = \bot$. By an application of Lemma A.6(2) there are two possibilities:
    - Either
      $$M \equiv N \mid n[(x)_w.P]^{\nu_n}_{t_n} = \prod_i n_i[W_i]^{\nu_i}_{t_i} \mid n[(x)_w.P]^{\nu_n}_{t_n} \ .$$
      In this case, by Lemma A.6(3) it follows that $\mathsf{actsnd}(N') \subseteq \mathsf{actsnd}(N)$. Thus $\mid \mathsf{actsnd}(N') \cap \nu_n \mid > 1$ implies $\mid \mathsf{actsnd}(N) \cap \nu_n \mid > 1$. Since M is transmission consistent it follows that $w = \bot$.

$*$ Or

$$M \equiv N \mid n[W]_{t_n}^{\nu_n} = \prod_i n_i[W_i]_{t_i}^{\nu_i} \mid n[W]_{t_n}^{\nu_n}$$

where W is either a receiver or a receiver with timeout, and $w = \bot$. □

Proof of Theorem 3.4
The proof follows by an application of Propositions A.3, A.4, A.7, and A.8. □

Proof of Theorem 6.3
We prove that the relation

$$\mathcal{S} \stackrel{\text{def}}{=} \{\big(M \mid O\,,\, N \mid O\big) : M \approx N,\ \ M \mid O \text{ and } N \mid O \text{ well-formed } \}$$

is a bisimulation by a case analysis.

- Since $M \approx N$ by definition of bisimilarity it follows $\mathsf{nds}(M) = \mathsf{nds}(N)$. This implies $\mathsf{nds}(M \mid O) = \mathsf{nds}(N \mid O)$.

- Let $M \mid O \xrightarrow{m!v \triangleright \nu} \widehat{M}$, by an application of rule (Out) because $M \mid O \xrightarrow{m!v} \widehat{M}$, with $\nu = \mathsf{ngh}(m, M \mid O) \setminus \mathsf{nds}(M \mid O) \neq \emptyset$. There are two possible cases:

  - $M \mid O \xrightarrow{m!v} \widehat{M}$ by an application of rule (Sync) because $M \xrightarrow{m!v} M'$ and $O \xrightarrow{m?v} O'$, with $\widehat{M} = M' \mid O'$. Since $M \xrightarrow{m!v} M'$ it follows that $m \in \mathsf{nds}(M)$ and hence $\nu = (\mathsf{ngh}(m, M) \setminus \mathsf{nds}(M)) \setminus \mathsf{nds}(O)$. Let $\nu' := \mathsf{ngh}(m, M) \setminus \mathsf{nds}(M)$, since $\nu \neq \emptyset$ it follows that $\nu' \neq \emptyset$. By an application of rule (Out) we have $M \xrightarrow{m!v \triangleright \nu'} M'$. Now, since $M \approx N$ there is N' such that $N \xRightarrow{m!v \triangleright \nu'} N'$ with $M' \approx N'$ and $\nu' = \mathsf{ngh}(m, N) \setminus \mathsf{nds}(N) \neq \emptyset$. Since the action $m!v \triangleright \nu'$ can be generated only by an application of rule (Out), there are N_1 and N_2 such that

    $$N \xrightarrow{\tau}{}^{*} N_1 \xrightarrow{m!v} N_2 \xrightarrow{\tau}{}^{*} N' \ .$$

    Since $O \xrightarrow{m?v} O'$, by several applications of Lemma 6.1 and one application of rule (Sync) we have:

    $$N \mid O \xrightarrow{\tau}{}^{*} N_1 \mid O \xrightarrow{m!v} N_2 \mid O' \xrightarrow{\tau}{}^{*} N' \mid O' \ .$$

    As

    $$\begin{array}{rcl} \nu & = & \mathsf{ngh}(m, M \mid O) \setminus \mathsf{nds}(M \mid O) \\ & = & (\mathsf{ngh}(m, M) \setminus \mathsf{nds}(M)) \setminus \mathsf{nds}(O) \\ & = & (\mathsf{ngh}(m, N) \setminus \mathsf{nds}(N)) \setminus \mathsf{nds}(O) \\ & = & \mathsf{ngh}(m, N \mid O) \setminus \mathsf{nds}(N \mid O) \\ & \neq & \emptyset \ . \end{array}$$

by an application of rule (Out) we can derive

$$N \mid O \xrightarrow{\tau}{}^{*} N_1 \mid O \xrightarrow{m!v \triangleright \nu} N_2 \mid O' \xrightarrow{\tau}{}^{*} N' \mid O' \ .$$

By Theorem 3.4, both $M' \mid O'$ and $N' \mid O'$ are well-formed. As $M' \approx N'$ it follows that $\left(M' \mid O' \, , \, N' \mid O'\right) \in \mathcal{S}$.

– $M \mid O \xrightarrow{m!v} \widehat{M}$, by an application of rule (Sync), because $M \xrightarrow{m?v} M'$ and $O \xrightarrow{m!v} O'$, with $\widehat{M} = M' \mid O'$. Since $O \xrightarrow{m!v} O'$, it follows that $m \in \mathsf{nds}(O)$ and hence $\nu = (\mathsf{ngh}(m, O) \setminus \mathsf{nds}(O)) \setminus \mathsf{nds}(M)$. Since $M \approx N$ there is N' such that $N \xRightarrow{m?v} N'$ with $M' \approx N'$. By several applications of Lemma 6.1 and one application of rule (Sync) it follows that:

$$N \mid O \xrightarrow{\tau}{}^{*} N_1 \mid O \xrightarrow{m!v} N_2 \mid O' \xrightarrow{\tau}{}^{*} N' \mid O' \ .$$

By definition of bisimilarity, $M \approx N$ implies $\mathsf{nds}(M) = \mathsf{nds}(N)$. Moreover, since $M \mid O$ and $N \mid O$ are well-formed and $m \in \mathsf{nds}(O)$, by node uniqueness it follows that $m \notin \mathsf{nds}(M)$ and $m \notin \mathsf{nds}(N)$. Thus,

$$\begin{array}{rcl} \mathsf{ngh}(m, N \mid O) \setminus \mathsf{nds}(N \mid O) & = & (\mathsf{ngh}(m, O) \setminus \mathsf{nds}(O)) \setminus \mathsf{nds}(N) \\ & = & (\mathsf{ngh}(m, O) \setminus \mathsf{nds}(O)) \setminus \mathsf{nds}(M) \\ & = & \mathsf{ngh}(m, M \mid O) \setminus \mathsf{nds}(M \mid O) \\ & = & \nu \\ & \neq & \emptyset \ . \end{array}$$

With this premise, by an application of rule (Out) we can derive

$$N \mid O \xrightarrow{\tau}{}^{*} N_1 \mid O \xrightarrow{m!v \triangleright \nu} N_2 \mid O' \xrightarrow{\tau}{}^{*} N' \mid O' \ .$$

By Theorem 3.4, both $M' \mid O'$ and $N' \mid O'$ are well-formed. As $M' \approx N'$ it follows that $\left(M' \mid O' \, , \, N' \mid O'\right) \in \mathcal{S}$.

- Let $M \mid O \xrightarrow{\tau} \widehat{M}$, by an application of rule (Shh), because $M \mid O \xrightarrow{m!v} \widehat{M}$ and $\mathsf{ngh}(m, M \mid O) \subseteq \mathsf{nds}(M \mid O)$. There are two possible cases:

  – Let $M \mid O \xrightarrow{m!v} \widehat{M}$, by an application of rule (Sync), because $M \xrightarrow{m!v} M'$ and $O \xrightarrow{m?v} O'$, with $\widehat{M} = M' \mid O'$ and

  $$\mathsf{ngh}(m, M \mid O) \setminus \mathsf{nds}(M \mid O) = (\mathsf{ngh}(m, M) \setminus \mathsf{nds}(M)) \setminus \mathsf{nds}(O) = \emptyset \ .$$

  Again there are two possibilities:

* Let $\mathsf{ngh}(m, M) \setminus \mathsf{nds}(M) = \emptyset$. Then, by an application of rule (Shh) we have $M \xrightarrow{\tau} M'$. Since $M \approx N$ there is N' such that $N \Rightarrow N'$ and $M' \approx N'$. We know that $O \xrightarrow{m?v} O'$. Let us assume $O \neq \mathbf{0}$ (the case when $O = \mathbf{0}$ is simple). In a network composed by several parallel components the action $m?v$ can be derived only by an application of rule (RcvPar). By definition of our networks there are n_i, W_i, ν_i, and t_i, for $1 \leq i \leq k$, such that $O = \prod_{i=1}^{k} n_i[W_i]_{t_i}^{\nu_i}$. By definition of rule (RcvPar), $O \xrightarrow{m?v} O'$ if and only if for all i, $1 \leq i \leq k$, there are W_i', ν_i', and t_i' such that

$$n_i[W_i]_{t_i}^{\nu_i} \xrightarrow{m?v} n_i[W_i']_{t_i'}^{\nu_i'}$$

and $O' = \prod_{i=1}^{k} n_i[W_i']_{t_i'}^{\nu_i'}$. Since $M \mid O$ is well-formed, by node-uniqueness it follows that $n_i \notin \mathsf{nds}(M)$ for all i, $1 \leq i \leq k$. Now, since

  - $\mathsf{ngh}(m, M) \setminus \mathsf{nds}(M) = \emptyset$
  - $n_i \notin \mathsf{nds}(M)$, for all i
  - $M \mid O$ is connected (see clause 1 of Definition 2.4)

it follows that $m \notin \nu_i$, for all i, $1 \leq i \leq k$. This implies that the transitions

$$n_i[W_i]_{t_i}^{\nu_i} \xrightarrow{m?v} n_i[W_i']_{t_i'}^{\nu_i'}$$

can only be derived by applying rule (OutRng) with $W_i' = W_i$, $\nu_i' = \nu_i$, and $t_i' = t_i$. This implies $O' = O$. Now, since $N \Rightarrow N'$, by several applications of Lemma 6.1 it follows that $N \mid O \Rightarrow N' \mid O = N' \mid O'$. By Theorem 3.4, both $M' \mid O'$ and $N' \mid O'$ are well-formed. As $M' \approx N'$ it follows that $\big(M' \mid O' \,,\, N' \mid O'\big) \in \mathcal{S}$.

* Let $\nu' = \mathsf{ngh}(m, M) \setminus \mathsf{nds}(M) \neq \emptyset$. Then, by an application of rule (Out) we have $M \xrightarrow{m!v \triangleright \nu'} M'$ because $M \xrightarrow{m!v} M'$. Since $M \approx N$ there is N' such that $N \xRightarrow{m!v \triangleright \nu'} N'$, with $M' \approx N'$ and $\nu' = \mathsf{ngh}(m, N) \setminus \mathsf{nds}(N)$. Since the action $m!v \triangleright \nu'$ can be only generated by an application of rule (Out), there are N_1 and N_2 such that

$$N \xrightarrow{\tau}{}^{*} N_1 \xrightarrow{m!v} N_2 \xrightarrow{\tau}{}^{*} N' \ .$$

Since $O \xrightarrow{m?v} O'$, by several applications of Lemma 6.1 and one application of rule (Sync) we have:

$$N \mid O \xrightarrow{\tau}{}^{*} N_1 \mid O \xrightarrow{m!v} N_2 \mid O' \xrightarrow{\tau}{}^{*} N' \mid O' \ .$$

As $M \mid O$ is well-formed and $m \in \mathsf{nds}(M)$, by node-uniqueness it follows that $m \notin \mathsf{nds}(O)$. Thus,

$$\begin{array}{rcl} \mathsf{ngh}(m, N \mid O) \setminus \mathsf{nds}(N \mid O) & = & (\mathsf{ngh}(m, N) \setminus \mathsf{nds}(N)) \setminus \mathsf{nds}(O) \\ & = & \nu' \setminus \mathsf{nds}(O) \\ & = & (\mathsf{ngh}(m, M) \setminus \mathsf{nds}(M)) \setminus \mathsf{nds}(O) \\ & = & \mathsf{ngh}(m, M \mid O) \setminus \mathsf{nds}(M \mid O) \\ & = & \emptyset \ . \end{array}$$

By an application of rule (Shh) we can derive

$$N \mid O \xrightarrow{\tau}{}^{*} N_1 \mid O \xrightarrow{\tau} N_2 \mid O' \xrightarrow{\tau}{}^{*} N' \mid O' \ .$$

By Theorem 3.4, both $M' \mid O'$ and $N' \mid O'$ are well-formed. As $M' \approx N'$ it follows that $\left(M' \mid O' \, , \, N' \mid O'\right) \in \mathcal{S}$.

– Let $M \mid O \xrightarrow{m!v} \widehat{M}$, by an application of rule (Sync) because $M \xrightarrow{m?v} M'$ and $O \xrightarrow{m!v} O'$, with $\widehat{M} = M' \mid O'$. This case is similar to a previous one.

- Let $M \mid O \xrightarrow{m?v} \widehat{M}$, by an application of rule (RcvPar), because $M \xrightarrow{m?v} M'$, $O \xrightarrow{m?v} O'$, and $\widehat{M} = M' \mid O'$. This case is easy.

- Let $M \mid O \xrightarrow{\sigma} \widehat{M}$ by an application of rule (Par-σ) because $M \xrightarrow{\sigma} M'$, $O \xrightarrow{\sigma} O'$, and $\widehat{M} = M' \mid O'$. This case is easy.

□