

# Observables for Mobile and Wireless Broadcasting Systems

Jens Chr. Godskesen

► **To cite this version:**

Jens Chr. Godskesen. Observables for Mobile and Wireless Broadcasting Systems. 12th International Conference on Coordination Models and Languages (COORDINATION) Held as part of International Federated Conference on Distributed Computing Techniques (DisCoTec), Jun 2010, Amsterdam, Netherlands. pp.1-15, 10.1007/978-3-642-13414-2\_1 . hal-01054627

**HAL Id: hal-01054627**

**<https://hal.inria.fr/hal-01054627>**

Submitted on 7 Aug 2014

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



# Observables for Mobile and Wireless Broadcasting Systems

Jens Chr. Godskesen \*

IT University of Copenhagen

**Abstract.** We discuss the presence of localities in observables for process calculi for mobile and wireless broadcasting systems in the context of weak barbed congruences and demonstrate that observability of the locality of a broadcasting node may be unsuitable when abstracting from node mobility, a natural abstraction current calculi agree upon. The discussion is carried out through a calculus  $bA\pi$ , a conservative extension of the Applied  $\pi$ -calculus and a contribution of its own. Through examples we demonstrate the applicability of  $bA\pi$  and its weak reduction congruence, where the locality of a broadcasting node is not observable, and we prove our bisimulation equivalence to be a *sound* and *complete* co-inductive characterization of the weak reduction congruence.

## 1 Introduction

Recently we have seen a large interest in the development of calculi for mobile and wireless broadcasting systems, e.g. CBS# [13], CMN [7], the  $\omega$ -calculus [16], and CMAN [5].<sup>1</sup> The calculi are defined with the purpose of being able to model and reason about a variety of types of systems spanning from ambient intelligence over mobile ad-hoc, sensor, and mesh networks, to cellular networks for mobile telephony. Because broadcasted messages will only reach the nodes within the communication range of the emitting node all the calculi have in common that the broadcast communication primitive is local (synchronous) broadcast. Also the calculi agree on letting nodes autonomously and arbitrarily change their neighbor relationship and thereby change the network topology. The calculi on the other hand differ on their neighborhood representations, in particular only in CMN the neighborhood relation is taken care of by a metric function that tells if two physical locations are close enough to communicate. The other calculi operate with logical locations without knowing physical distances but just the neighborhood relationships.

**Related Work** Often, as put forward in the seminal work on *barbed bisimulation* [12, 10], process calculi are equipped with a reduction semantics and

---

\* Supported by the VKR Centre of Excellence MT-LAB.

<sup>1</sup> CWS [9] and TWCS [8] also consider wireless broadcasting systems but they do not cater for node mobility.

a reduction congruence where the latter is based on some kind of observables (barbs). The idea is to strive for a simple reduction semantics and to allow an external observer to observe the system through a limited set of *barbs*. Indistinguishability under these observations gives rise to a natural equivalence which in turn induces a natural congruence, i.e. the equivalence in all contexts closed under structural congruence.

In non-broadcasting calculi for mobility, like e.g. the  $\pi$ -calculus [15, 11], an observable is a (channel) *name* on which a message is transmitted (or received), or as for the Ambient-calculus [2] a barb is a name indicating the presence of an (unrestricted) top-level ambient. For non-broadcasting calculi for mobile and distributed computing with localities, like  $D\pi$  [14], the barbs are related to specific locations, say sending out a message on a channel at a specific node. For TKLAIM [3] it is shown that the observables for Ambients and  $D\pi$  have the same discriminating power.

However, as also addressed in [9], it seems to be not obvious to decide what an adequate observable for mobile and local wireless broadcasting calculi should be. One of the problems being that in a network of mobile wireless broadcasting devices each has a location and a transmission range and it is not immediate how to take location and range into account when defining the observables. In CBS# for instance the observables for a network  $N$  are pairs consisting of a data term  $t$  and a locality (node) name  $l$ . Intuitively the observable here means that  $N$  is capable of storing  $t$  at location  $l$  (and hence later  $l$  may broadcast  $t$ ). In CMN an observable for a network  $N$  is a pair, an output channel  $n$  and a set of node locations  $L$ . Intuitively a barb means that any location in  $L$  is within metric distance of the transmitting range of the emitting node and hence can receive a message on input channel  $n$ . In CMAN an observable is the name of the location of the broadcasting node, and also in TWCS [8] a node locality is always part of a barb.<sup>2</sup> Hence, to our knowledge all contemporary process calculi for mobile and wireless broadcasting systems, which do not employ a metric to measure the physical distance between nodes but operates with logical locations, adopt the legacy from non-broadcasting calculi for localized and distributed computing, like  $D\pi$  and TKLAIM, and let the locality of the broadcasting node be part of their barbs.

**Motivation** In this paper we discuss observables for local synchronous broadcast mobile systems, and in particular we demonstrate that observability of the (logical) locality of a broadcasting node may be unsuitable for a semantics that abstracts from node mobility, a natural abstraction all the calculi mentioned above agree upon. The source of our discussion is a broadcast calculus,  $bA\pi$ , inspired by and a conservative extension of the Applied  $\pi$ -calculus [1]. We consider  $bA\pi$  a contribution of its own since to our knowledge it is the first calculus for

---

<sup>2</sup> The  $\omega$ -calculus [16] does not offer an explicit definition of observables, but since it is a conservative extension of the  $\pi$ -calculus we would expect that the set of observables for the  $\omega$ -calculus at least contains the observables of the  $\pi$ -calculus.

mobile and wireless local broadcasting systems that allows for reasoning about an unbounded number of nodes. The calculus is briefly outlined below.

A *node*,  $\lfloor p \rfloor_l$ , in  $bA\pi$  is a *process*  $p$  located at some (logical) *location*  $l$ . Nodes composed in parallel constitute a *network*, say  $\lfloor p \rfloor_k \parallel \lfloor q \rfloor_l \parallel \lfloor r \rfloor_m$ . Processes at the same location  $l$  may communicate on a name  $n$ , for example

$$\lfloor \bar{n}\langle t \rangle.p \rfloor_l \parallel \lfloor n(x).q \rfloor_l \longrightarrow \lfloor p \rfloor_l \parallel \lfloor q\{t/x\} \rfloor_l \quad (1)$$

where  $q\{t/x\}$  is  $q$  with all free occurrences of  $x$  replaced by  $t$ . Connectivity between nodes is represented by an annotation, for instance

$$\lfloor p \rfloor_l \parallel \lfloor q \rfloor_m \parallel \{l \mapsto m\} \ , \quad (2)$$

where  $l$  is connected to  $m$  but not vice versa. We enforce unidirectional instead of bidirectional links between nodes which seems to be more natural for wireless systems. Following the ideas in [13, 7, 16, 5]<sup>3</sup> mobility is defined by a simple reduction, say that the node at location  $m$  in (2) autonomously moves and becomes *connected* to the node at location  $l$ ,

$$\lfloor p \rfloor_l \parallel \lfloor q \rfloor_m \parallel \{l \mapsto m\} \longrightarrow \lfloor p \rfloor_l \parallel \lfloor q \rfloor_m \parallel \{l \mapsto m\} \parallel \{m \mapsto l\} \ .$$

Dually, nodes may arbitrarily *disconnect*, for instance  $l$  disconnects from  $m$  in

$$\lfloor p \rfloor_l \parallel \lfloor q \rfloor_m \parallel \{l \mapsto m\} \parallel \{m \mapsto l\} \longrightarrow \lfloor p \rfloor_l \parallel \lfloor q \rfloor_m \parallel \{m \mapsto l\} \ .$$

A process  $\langle t \rangle.p$  can broadcast  $t$  and in so doing become  $p$ , and a process  $(x).q$  can receive a broadcasted message  $t$  becoming  $q\{t/x\}$ . *Local synchronous broadcast* is defined by a *broadcast reduction*, say

$$\begin{aligned} & \lfloor \langle t \rangle.p \rfloor_l \parallel \{m \mapsto l\} \parallel \{n \mapsto l\} \parallel \lfloor (x).q \rfloor_m \parallel \lfloor (x).r \rfloor_n \\ & \longrightarrow \lfloor p \rfloor_l \parallel \{m \mapsto l\} \parallel \{n \mapsto l\} \parallel \lfloor q\{t/x\} \rfloor_m \parallel \lfloor r\{t/x\} \rfloor_n \ , \end{aligned}$$

where  $\langle t \rangle.p$  broadcasts to nodes connected to  $l$ , but messages may be lost.

Names may be restricted and in particular we may let a location be unique as in  $\nu l.\lfloor p \rfloor_l$ . Also, we allow for an unbounded number of nodes, as in  $!\nu l.\lfloor p \rfloor_l$ , which is a novelty compared to the current calculi for mobility and local broadcast where one is only allowed to reason about a finite number of network nodes.

Due to the reduction (1) where processes at the same location communicate the context  $\lfloor n(x).\bar{m}\langle x \rangle \rfloor_l$  can distinguish  $\lfloor \bar{n}\langle t \rangle \rfloor_l$  from  $\nu l.\lfloor \bar{n}\langle t \rangle \rfloor_l$  and from  $\lfloor \bar{n}\langle t \rangle \rfloor_k$  if  $l \neq k$ , so it seems natural that  $\lfloor \bar{n}\langle t \rangle \rfloor_l$ ,  $\lfloor \bar{n}\langle t \rangle \rfloor_k$ , and  $\nu l.\lfloor \bar{n}\langle t \rangle \rfloor_l$  must be considered pairwise inequivalent even in a weak setting where mobility is ignored. But what about  $\lfloor \langle t \rangle \rfloor_l$ ,  $\lfloor \langle t \rangle \rfloor_k$ , and  $\nu l.\lfloor \langle t \rangle \rfloor_l$ ? As it will turn out the three nodes are pairwise inequivalent when mobility is taken into account, but when mobility is abstracted one may argue that they should be considered indistinguishable,

<sup>3</sup> Arbitrary mobility is an over approximation and more realistic mobility models are considered in [6].

intuitively because any node can move and connect to any (even a new) locality and receive the broadcasted message. For instance we have

$$[\langle t \rangle]_l \parallel [(x).\overline{m}\langle x \rangle]_k \parallel \{k \mapsto l\} \longrightarrow [0]_l \parallel [\overline{m}\langle t \rangle]_k \parallel \{k \mapsto l\}$$

and in a weak setting we can obtain a similar computation for  $\nu l. [\langle t \rangle]_l$  in the same context by letting:

$$\begin{aligned} \nu l. [\langle t \rangle]_l \parallel [(x).\overline{m}\langle x \rangle]_k \parallel \{k \mapsto l\} &\equiv \nu l'. ([\langle t \rangle]_{l'} \parallel [(x).\overline{m}\langle x \rangle]_k \parallel \{k \mapsto l\}) \\ &\longrightarrow \nu l'. ([\langle t \rangle]_{l'} \parallel [(x).\overline{m}\langle x \rangle]_k \parallel \{k \mapsto l\} \parallel \{k \mapsto l'\}) \\ &\longrightarrow \nu l'. ([0]_{l'} \parallel [\overline{m}\langle t \rangle]_k \parallel \{k \mapsto l\} \parallel \{k \mapsto l'\}) \\ &\longrightarrow \nu l'. ([0]_{l'} \parallel [\overline{m}\langle t \rangle]_k \parallel \{k \mapsto l\}) \equiv \nu l. [0]_l \parallel [\overline{m}\langle t \rangle]_k \parallel \{k \mapsto l\} \end{aligned}$$

Notice that an observable identifying the locality of the broadcasting entity clearly will distinguish the three nodes  $[\langle t \rangle]_l$ ,  $[\langle t \rangle]_k$ , and  $\nu l. [\langle t \rangle]_l$ , so it may be too strict a barb.

Below we discuss and compare three kinds of barbs: the observability of *i*) output on a name at a given location, *ii*) broadcast of a name at some location, and *iii*) the broadcasting location respectively. For the three congruences induced by each of these barbs we show that the two former coincide and strictly contain the latter in a weak setting where one reduction may be matched by zero or more reductions, and for the corresponding strong congruences where a reduction must be matched by precisely one reduction all three congruences coincide. To illustrate the suitability of  $bA\pi$  we provide a labelled operational semantics and give a sound and complete co-inductive characterization of the largest weak congruences mentioned above. Also we give a larger example of a route-request protocol that could not have been modelled in the calculi presented in [13, 7, 16, 5] because it contains an unbounded number of nodes.

The paper is organized as follows:  $bA\pi$  is presented in Section 2. The barbs, the reduction semantics, and the barbed congruences are defined and compared in Section 3. The sound and complete co-inductive labelled operational semantics is provided in Section 4. Finally we close by a conclusion.

## 2 The Calculus

The syntax of our calculus  $bA\pi$  is outlined below defining first terms, then processes, and finally networks and extended networks.

We assume a *signature*  $\Sigma$  with a finite set of function symbols  $f$  each with an arity. Also we assume an infinite set of *names*  $\mathcal{N}$  ranged over by  $n$ , an infinite set of *variables*  $\mathcal{X}$  ranged over by  $x$ . Then the set of *terms* ranged over by  $s$  and  $t$  is defined by the grammar below where  $f$  is a function symbol with arity  $k$ .

$$t ::= n \mid x \mid f(t_1, \dots, t_k)$$

We let  $s\{t/x\}$  denote  $s$  where  $x$  is substituted by  $t$ . We let  $\mathcal{T}$  denote the set of all terms and let  $\hat{t}$  range over *ground* terms with no variables.<sup>4</sup>

<sup>4</sup> For a discussion about associating sorts with terms we refer the reader to [1].

The set of *processes* ranged over by  $p, q$ , and  $r$  is defined by the grammar:

$$p ::= 0 \mid \langle t \rangle.p \mid \bar{n}(t).p \mid (x).p \mid u(x).p \mid \text{if } (t = s) \text{ then } p \text{ else } q \mid \nu n.p \mid p \parallel q \mid !p$$

where  $u$  ranges over variables and names. The processes  $0, \nu n.p, p \parallel q, !p$  (replication), and  $\text{if } (t = s) \text{ then } p \text{ else } q$ , are standard. The process  $\langle t \rangle.p$  may broadcast  $t$  and in so doing become  $p$ ,  $\bar{n}(t).p$  may send  $t$  on channel  $n$  (unicast),  $(x).p$  binds  $x$  in  $p$  and may receive a broadcasted term  $t$  and replace all free occurrences of  $x$  in  $p$  by  $t$ , likewise  $n(x).p$  binds  $x$  in  $p$  and may receive a term  $t$  sent on channel  $n$ . As usual we often leave out a trailing  $0$ .

We let  $p\{t/x\}$  denote  $p$  where  $x$  is substituted by  $t$ , taking care to avoid clash of variables and names using  $\alpha$ -conversion if needed. The set of *free names* in  $p$  is denoted by  $fn(p)$ , and its *free variables* are denoted by  $fv(p)$ .

The set of *networks* ranged over by  $P$  and  $Q$  is defined by the grammar:

$$P ::= 0 \mid [p]_l \mid \{l \mapsto m\} \mid \nu n.P \mid P \parallel Q \mid !P$$

The network  $0$  denotes the empty network.  $[p]_l$  is a node at location  $l$  containing the process  $p$ .  $\{l \mapsto m\}$  tells that the node at location  $l$  is connected to node  $m$ .  $\nu n.P$  is the network  $P$  with a new name bound by  $n$ ,  $P \parallel Q$  is the parallel composition of the two networks  $P$  and  $Q$ , and  $!P$  denotes an unbounded number of parallel compositions of the network  $P$ .

We extend networks with *variable restrictions* and *active substitutions*,  $\{t/x\}$ , and we let a *frame*,  $\phi$ , be the static part of a process. Frames, extended processes, and extended networks are defined by the following grammar:

$$\begin{aligned} \phi &::= 0 \mid \{t/x\} \mid \nu u.\phi \mid \phi \parallel \phi \\ e &::= p \mid \{t/x\} \mid \nu u.e \mid e \parallel e \\ E &::= P \mid [e]_n \mid \nu u.E \mid E \parallel E \end{aligned}$$

We let the new name (variable) operator have higher precedence than the left associative parallel composition.

Intuitively an active substitution  $\{t/x\}$  is like an ordinary substitution that floats and may be applied to any process that comes into contact with it. If we control the floating of an active substitution by restricting its variable it may be interpreted as:  $[let\ x = t\ in\ p]_l \stackrel{\text{def}}{=} [\nu x.(\{t/x\} \parallel p)]_l$ .

The sets of free names and variables in  $E$ , denoted by  $fn(E)$  and  $fv(E)$  respectively, are defined as expected. In particular  $fn(\{t/x\}) = fn(t)$  and  $fv(\{t/x\}) = \{x\} \cup fv(t)$ . We let  $E\{t/x\}$  denote  $E$  where all free occurrences of  $x$  in  $E$  are substituted by  $t$ . The *domain* at a free location  $l$  of  $E$ , denoted by  $dom_l(E)$ , is the set of variables for which  $E$  contains a substitution  $\{t/x\}$  at location  $l$  not under  $\nu x$ . The domain of  $E$ , denoted by  $dom(E)$  is the union of  $dom_l(E)$  for all free locations  $l$  in  $E$ . We say that  $dom(E) = dom(F)$  if  $dom_l(E) = dom_l(F)$  for all  $l$ .  $E$  is *closed* when  $fv(E) \subseteq dom(E)$ .

For a finite index set  $I$  we let  $\prod_{i \in I} E_i$  denote the parallel composition of  $E_i$  for all  $i \in I$ , if  $I = \emptyset$  then  $\prod_{i \in I} E_i$  is  $0$ . We shall write  $\tilde{u}$  for a disjoint sequence

|  |   |  |
|--|---|--|
| $[\nu u.p]_l \equiv \nu u.[p]_l$ , if $u \neq l$                   | $[!p]_l \equiv ![p]_l$  | $[p \parallel q]_l \equiv [p]_l \parallel [q]_l$                       |
| $[p \parallel 0]_l \equiv [p]_l$                                   | $[\{t/x\}]_l \equiv [\{s/x\}]_l$ , if $s = t$   |  |
| $[\nu x.\{t/x\}]_l \equiv [0]_l$                                   | $[\{t/x\} \parallel e]_l \equiv [\{t/x\} \parallel e\{t/x\}]_l$                         |  |
| $\{l \mapsto k\} \equiv \{l \mapsto k\} \parallel \{l \mapsto k\}$ | $[(x).p \parallel (x).q]_l \equiv [(x).(p \parallel q)]_l$                              |  |
| $E \parallel 0 \equiv E$   | $E \parallel E' \equiv E' \parallel E$  | $(E \parallel E') \parallel E'' \equiv E \parallel (E' \parallel E'')$ |
| $\nu u.\nu v.E \equiv \nu v.\nu u.E$                               | $\nu u.E \parallel E' \equiv \nu u.(E \parallel E')$ , if $u \notin fn(E') \cup fv(E')$ |  |

**Table 1.** Structural congruence.

of either names or variables and  $u \in \tilde{u}$  if  $u$  occurs in the sequence  $\tilde{u}$ . We let  $\tilde{u}\tilde{v}$  denote the concatenation of disjoint sequences. Sometimes we write  $(u_k)_{k \in \tilde{v}}$  to denote a disjoint sequence indexed by the elements in  $\tilde{v}$ . Whenever  $\tilde{t} = (t_x)_{x \in \tilde{x}}$  we write  $\{\tilde{t}/\tilde{x}\}$  for  $\prod_{x \in \tilde{x}} \{t_x/x\}$ . We write  $\{\tilde{n} \mapsto l\}$  and  $\{l \mapsto \tilde{n}\}$  for  $\prod_{n \in \tilde{n}} \{n \mapsto l\}$  and  $\prod_{n \in \tilde{n}} \{l \mapsto n\}$  respectively.

We say that a  $E$  is *well-formed* if  $E$  contains at most one substitution for each variable and exactly one when the variable is restricted. Also, for a well-formed  $E$  we assume substitutions are cycle-free and we presuppose that a free variable at a location  $l$  is contained in  $dom_l(E)$ . In the sequel we consider only networks in the set of well-formed extended networks  $\mathbf{N}$  and we identify networks up to  $\alpha$ -equivalence. The set of well-formed and closed networks is denoted by  $\mathbf{N}_c$ .

### 3 Reduction Semantics

In this section we provide our calculus with a natural reduction semantics.

Given a signature we equip it with an equational theory and we write  $\Sigma \vdash s = t$  when the equation is in the theory associated with  $\Sigma$ . Often  $\Sigma$  is left implicit writing  $s = t$  for  $\Sigma \vdash s = t$ . Here we refrain from explicitly treating a sort system for terms, implicitly assume terms are well-sorted, and refer the reader to [1].

We write  $C(E)$  for the insertion of  $E$  in the hole of a variable closing network context  $C$  and say that relation  $\mathcal{R}$  on  $\mathbf{N}$  is a *congruence* if  $E \mathcal{R} E'$  implies  $C(E) \mathcal{R} C(E')$  for any  $C$ . Structural congruence on  $\mathbf{N}$ ,  $\equiv$ , is the least congruence and equivalence relation that is closed under  $\alpha$ -conversion and the rules in Table 1. Almost all the rules in Table 1 are standard, but notice that the axiom  $[(x).p \parallel (x).q]_l \equiv [(x).(p \parallel q)]_l$  captures that a broadcasted message may have multiple simultaneous receivers within the same location. Also we allow to collapse multiple occurrences of the same connectivity information. From [1] we adopt the rule  $[\{t/x\} \parallel e]_l \equiv [\{t/x\} \parallel e\{t/x\}]_l$ , capturing the essence of active substitutions, and we are always allowed to introduce arbitrary new substitutions at a location as introduced by  $[\nu x.\{t/x\}]_l \equiv [0]_l$ .

|   |  |
|---|--|
| $(rep) \frac{}{!E \longrightarrow E \parallel !E}$  | $(if) \frac{}{[if (t = t) \text{ then } p \text{ else } q]_l \longrightarrow [p]_l}$ |
| $(else) \frac{}{[if (\hat{t} = \hat{s}) \text{ then } p \text{ else } q]_l \longrightarrow [q]_l} \quad \hat{t} \neq \hat{s}$   |  |
| $(com) \frac{}{[\bar{n}\langle \hat{t} \rangle.p \parallel n(x).q]_l \longrightarrow [p \parallel q\{\hat{t}/x\}]_l}$   |  |
| $(brd) \frac{}{[\langle \hat{t} \rangle.p]_l \parallel \prod_{k \in \tilde{n}} [(x).q_k]_k \parallel \{\tilde{n} \mapsto l\} \longrightarrow [p]_l \parallel \prod_{k \in \tilde{n}} [q_k\{\hat{t}/x\}]_k \parallel \{\tilde{n} \mapsto l\}}$ |  |
| $(con) \frac{}{0 \longrightarrow \{l \mapsto k\}}$  | $(dis) \frac{}{\{l \mapsto k\} \longrightarrow 0}$                                   |

**Table 2.** Reduction rules, networks.

*Example 1.* Similar to [1] we have  $[\langle t \rangle.p]_l \equiv \nu x. [\{t/x\} \parallel \langle x \rangle.p]_l$ , assuming  $x \notin fv(\langle t \rangle.p)$ , because:

$$\begin{aligned} [\langle t \rangle.p]_l &\equiv [\langle t \rangle.p] \parallel 0 \equiv [\langle t \rangle.p \parallel \nu x.\{t/x\}]_l \equiv \nu x. [\{t/x\} \parallel \langle t \rangle.p]_l \\ &\equiv \nu x. [\{t/x\} \parallel (\langle x \rangle.p)\{t/x\}]_l \equiv \nu x. [\{t/x\} \parallel \langle x \rangle.p]_l \end{aligned}$$

We define the reduction relation,  $\longrightarrow$ , as the least relation on  $\mathbf{N}$  closed under  $\equiv$ , new names, variables, and parallel composition, and satisfying the rules in Table 2. The rules *(rep)*, *(if)*, *(else)*, and *(com)* are standard. The rule *(brd)* says that a process at a node may broadcast to (some of the) nodes right now connected to that node. The rules *(con)* and *(dis)* allows connection and disconnection between nodes respectively. Notice that nodes connected to an emitter may receive a broadcasted message (but the message may also be lost) whereas disconnected nodes do not have the possibility of reception.

**Strong Barbed Congruence** Next we introduce natural strong observational equivalence and congruence relations.

As motivated in the Introduction we are able to observe that a process at a (free) location is capable of sending on a (free) channel, hence the two nodes  $[\bar{n}\langle t \rangle]_l$  and  $[\bar{n}\langle t \rangle]_k$  should not be considered equivalent if  $k \neq l$  because the process  $n(x).\bar{m}\langle x \rangle$  when put at the physical location  $l$  can distinguish the two. Similar to  $D\pi$  we may therefore introduce a *barb* writing  $E \downarrow l_n$  when  $E \equiv \nu \tilde{u}.([\bar{n}\langle t \rangle.p]_l \parallel F)$  for some  $\tilde{u}$ ,  $t$ ,  $p$ , and  $F$  where  $l$  and  $n$  do not belong to  $\tilde{u}$ .



**Definition 1.** A symmetric relation  $\mathcal{R}$  on  $\mathbf{N}_c$  is a strong barbed congruence if it is a congruence and if  $E \mathcal{R} F$  implies  $\text{dom}(E) = \text{dom}(F)$ , and

$$E \longrightarrow E' \text{ implies } \exists F'. F \longrightarrow F' \text{ and } E' \mathcal{R} F'$$

$$E \downarrow l_n \text{ implies } F \downarrow l_n$$

$\simeq$  is the largest strong barbed congruence.

It is immediate that  $\simeq$  is an equivalence relation containing  $\equiv$ .

*Example 2.* Clearly  $0 \simeq \nu u.0 \simeq [0]_l$ , but also  $0 \simeq \nu n.[\bar{n}\langle t \rangle.p]_l \simeq \nu l.[\bar{n}\langle t \rangle.p]_l$ . Observe  $0 \simeq \nu l.[\phi]_l$  because  $\text{dom}(\nu l.[\phi]_l) = \emptyset$ .

Similar to [1] let  $f$  and  $g$  be two unary functions occurring in no equations. Further let, where  $n$  and  $m$  are distinct from  $l$ ,

$$E = [\nu n.\{n/x\} \parallel \nu m.\{m/y\}]_l$$

$$E' = \nu n.[\{g(n)/x\} \parallel \{f(n)/y\}]_l$$

$$F = \nu n.[\{n/x\} \parallel \{f(n)/y\}]_l$$

then  $E \simeq E'$  because in both  $E$  and  $E'$  the two variables  $x$  and  $y$  are mapped to two unrelated values that are different from any value any context can build. But,  $E \not\simeq F$  because the two may be distinguished by the node

$$[\text{if } (y = f(x)) \text{ then } \bar{n}\langle x \rangle]_l$$

*Example 3.* It turns out that  $\nu l.[\langle n \rangle]_l \not\simeq [\langle n \rangle]_l$  because for

$$C = (-) \parallel [(x).\bar{m}\langle x \rangle]_k \parallel \{k \mapsto l\}$$

we have  $C([\langle n \rangle]_l) \longrightarrow [0]_l \parallel [\bar{m}\langle n \rangle]_k \parallel \{k \mapsto l\} = E$  where  $E \downarrow k_m$  which cannot be matched by  $C(\nu l.[\langle n \rangle]_l)$ .

The observation in Example 3 gives rise to alternatively letting a barb be the observation of a broadcasting location, i.e.  $E \downarrow l$  when  $E \equiv \nu \tilde{u}.([\langle t \rangle.p]_l \parallel F)$  for some  $t, p, \tilde{u}$ , and  $F$  where  $l \notin \tilde{u}$ . Hence an environment  $\{k \mapsto l\} \parallel [(x).q]_k$  may observe a network with a barb  $\downarrow l$ .

**Definition 2.** A symmetric relation  $\mathcal{R}$  on  $\mathbf{N}_c$  is a strong location barbed congruence if it is a congruence and if  $E \mathcal{R} F$  implies  $\text{dom}(E) = \text{dom}(F)$ , and

$$E \longrightarrow E' \text{ implies } \exists F'. F \longrightarrow F' \text{ and } E' \mathcal{R} F'$$

$$E \downarrow l \text{ implies } F \downarrow k \text{ for some } k$$

$\simeq_{loc}$  is the largest strong location barbed congruence.

*Example 4.* Clearly  $\nu l.[\langle n \rangle]_l \not\simeq_{loc} [\langle n \rangle]_l$ . Observe that  $[\langle n \rangle]_l \not\simeq_{loc} [\langle n \rangle]_k$  if  $k \neq l$ . The reason why is that if it was the case that  $[\langle n \rangle]_l \simeq_{loc} [\langle n \rangle]_k$  then also, since  $\simeq_{loc}$  is a congruence (assuming without loss of generality that  $n \neq l$ ),  $\nu l.[\langle n \rangle]_l \simeq_{loc} \nu l.[\langle n \rangle]_k \equiv [\langle n \rangle]_k$  which as stated just before is not true.<sup>5</sup>

<sup>5</sup> Observe then that the second clause in Definition 2 can, without changing the meaning of the definition, be replaced by “ $E \downarrow l$  implies  $F \downarrow l$ ”.

Finally, we may let a barb be the observation of a broadcast message but without saying the broadcasting location. For simplicity we just use names as barbs and define  $E \downarrow \langle n \rangle$  when  $E \equiv \nu \tilde{u}.([\langle n \rangle.p]_l \parallel F)$  for some  $p, l, \tilde{u}$ , and  $F$  where  $n \notin \tilde{u}$  (but it may be that  $l \in \tilde{u}$ ). Hence, by first connecting to the (unknown) node broadcasting  $n$ , a context  $[(x).if (x = n) \text{ then } p]_k$  may observe a network with a barb  $\downarrow \langle n \rangle$ .

**Definition 3.** A symmetric relation  $\mathcal{R}$  on  $\mathbf{N}_c$  is a strong message barbed congruence if it is a congruence and if  $E \mathcal{R} F$  implies  $\text{dom}(E) = \text{dom}(F)$ , and

$$\begin{aligned} E \longrightarrow E' \text{ implies } \exists F'. F \longrightarrow F' \text{ and } E' \mathcal{R} F' \\ E \downarrow \langle n \rangle \text{ implies } F \downarrow \langle n \rangle \end{aligned}$$

$\simeq_{msg}$  is the largest strong message barbed congruence.

*Example 5.* Recall that  $[\langle n \rangle]_l \not\approx_{loc} [\langle n \rangle]_k$  if  $k \neq l$ , and interestingly, although the two nodes may broadcast the same message  $n$ , also  $[\langle n \rangle]_l \not\approx_{msg} [\langle n \rangle]_k$ , because letting for some fresh  $n'$

$$C = (-) \parallel \{m \mapsto l\} \parallel [(x).\langle n' \rangle]_m$$

then  $C([\langle n \rangle]_l) \longrightarrow [0]_l \parallel \{m \mapsto l\} \parallel [\langle n' \rangle]_m = E$  where  $E \downarrow \langle n' \rangle$  which cannot be matched by  $C([\langle n \rangle]_k)$ .

The three notions of strong barbed congruences turn out to be identical demonstrating the robustness of our notion of barbs.

**Theorem 1.**  $\simeq = \simeq_{loc} = \simeq_{msg}$

**Weak Barbed Congruence** Below we introduce a weak observational equivalence and congruence relation for each of the three kinds of barbs introduced above. The equivalence relations are weak in the standard sense that a reduction may be matched by zero or more reductions, and hence we then abstract from communication within the same location, broadcast communication between localities, and mobility.

Let  $\Longrightarrow$  be the reflexive and transitive closure of  $\longrightarrow$ . We write  $E \Downarrow b$  if  $E \Longrightarrow E'$  for some  $E'$  such that  $E' \downarrow b$  where  $b$  is one of the three kinds of barbs mentioned above.

**Definition 4.** A symmetric relation  $\mathcal{R}$  on  $\mathbf{N}_c$  is a weak barbed congruence if it is a congruence and if  $E \mathcal{R} F$  implies  $\text{dom}(E) = \text{dom}(F)$ , and

$$\begin{aligned} E \longrightarrow E' \text{ implies } \exists F'. F \Longrightarrow F' \text{ and } E' \mathcal{R} F' \\ E \downarrow l_n \text{ implies } F \Downarrow l_n \end{aligned}$$

$\cong$  is the largest weak barbed congruence.

Since changes in connectivity is unobservable for weak barbed congruence it follows that  $E \cong E \parallel \{l \mapsto k\}$ .

**Definition 5.** A symmetric relation  $\mathcal{R}$  on  $\mathbf{N}_c$  is a weak location barbed congruence if it is a congruence and if  $E \mathcal{R} F$  implies  $\text{dom}(E) = \text{dom}(F)$ , and

$$\begin{aligned} E \longrightarrow E' \text{ implies } \exists F'. F \Longrightarrow F' \text{ and } E' \mathcal{R} F' \\ E \downarrow l \text{ implies } F \downarrow k \text{ for some } k \end{aligned}$$

$\cong_{loc}$  is the largest weak location barbed congruence.

**Definition 6.** A symmetric relation  $\mathcal{R}$  on  $\mathbf{N}_c$  is a weak message barbed congruence if it is a congruence and if  $E \mathcal{R} F$  implies  $\text{dom}(E) = \text{dom}(F)$ , and

$$\begin{aligned} E \longrightarrow E' \text{ implies } \exists F'. F \Longrightarrow F' \text{ and } E' \mathcal{R} F' \\ E \downarrow \langle n \rangle \text{ implies } F \downarrow \langle n \rangle \end{aligned}$$

$\cong_{msg}$  is the largest weak message broadcast barbed congruence.

*Example 6.* For the same reason as explained in Example 4,  $\nu l. \lfloor \langle n \rangle \rfloor_l \not\cong_{loc} \lfloor \langle n \rangle \rfloor_l$  and when  $l \neq k$  also  $\lfloor \langle n \rangle \rfloor_l \not\cong_{loc} \lfloor \langle n \rangle \rfloor_k$ . But interestingly,  $\lfloor \langle n \rangle \rfloor_l \cong_{msg} \lfloor \langle n \rangle \rfloor_k$  and when  $n \neq l$  then  $\nu l. \lfloor \langle n \rangle \rfloor_l \cong_{msg} \lfloor \langle n \rangle \rfloor_l$  as discussed in the Introduction. We show this formally in the next section, confer Example 9 and 10.

The relationship between the strong and weak barbed congruences is illustrated by the following theorem.

**Theorem 2.**  $\simeq \subset \cong_{loc} \subset \cong_{msg} = \cong$ .

*Example 7.* The order of infinite repetitive broadcast sequences may be interchanged. E.g.  $\lfloor \langle n \rangle . \langle m \rangle \rfloor_l \cong_{msg} \lfloor \langle m \rangle . \langle n \rangle \rfloor_k$  because receivers may disconnect before a message is broadcasted and connect again in order to receive next.

*Example 8.* Suppose a simple route-request protocol with the purpose of finding out as to whether there exists a route from source to destination in a mobile ad-hoc network. In this simple example we do not cater to find the actual route, just knowledge about its existence is sufficient. We may model the protocol by

$$E_{k,k'} = \lfloor \nu n. \langle \text{pair}(req, n) \rangle . p \rfloor_l \parallel \lfloor r \rfloor_k \parallel \lfloor r \rfloor_{k'} \parallel \lfloor q \rfloor_m$$

where (using equations instead of replication)  $p$ ,  $q$ , and  $r$  are defined in Table 3 and the equational theory consists of  $\text{fst}(\text{pair}(x, y)) = x$  and  $\text{snd}(\text{pair}(x, y)) = y$ . Intuitively, the source at  $l$  sends out a request with a unique identifier  $n$ . The request is expected to reach its destination at  $m$  where a reply containing  $n$  is returned. The message may travel in a number of hops through the relay processes at  $k$  and  $k'$ . As in many realistic routing protocols for mobile ad-hoc networks a relay process forwards a request and maintains a thread waiting for a reply to it while continuing listening to new requests. When a reply with the right identifier appears it is simply forwarded and the waiting thread terminates.

If we can observe which location is about to broadcast then clearly  $E_{k,k'} \not\cong_{loc} E_{l,l'}$  if say  $k \neq l$  because the process at node  $k$  may receive the request after

|  |
|--|
| $p \stackrel{\text{def}}{=} (x).\text{if } (fst(x) = rep) \text{ then if } (snd(x) = n) \text{ then } \bar{a}\langle succ \rangle \text{ else } p \text{ else } p$ |
| $q \stackrel{\text{def}}{=} (x).\text{if } (fst(x) = req) \text{ then } \langle pair(rep, snd(x)) \rangle \text{ else } q$   |
| $r \stackrel{\text{def}}{=} (x).\text{if } (fst(x) = req) \text{ then } \langle x \rangle.r' \parallel r \text{ else } r$  |
| $r' \stackrel{\text{def}}{=} (y).\text{if } (fst(y) = rep) \text{ then if } (snd(y) = snd(x)) \text{ then } \langle y \rangle \text{ else } r' \text{ else } r'$   |

**Table 3.** Processes in the route-request protocol.

which it is able to forward it. However as discussed in the Introduction it may be too strong to allow for observing the actual locality about to broadcast, often as for the route-request protocol of this example it is more natural to be able to observe only the data broadcasted and not whom did the broadcast. For instance it turns out that  $E_{k,k'} \cong E_{l,\nu}$  and also that  $E_{k,k'} \cong F$ , where  $F$  is a network with an unbounded number of relay processes at unique locations, i.e.

$$F = [\nu n.\langle pair(req, n) \rangle.p]_l \parallel !\nu k.[r]_k \parallel [q]_m$$

We postpone the proof of our latter propositions to Example 12 in Section 4.

## 4 Labeled Operational Semantics

In this section we provide a labelled transition system semantics for extended networks based on which we give a sound and complete co-inductive bisimulation characterization of our weak barbed congruence from above.<sup>6</sup>

We define a set of *actions*  $\mathcal{A}$ , ranged over by  $\alpha$ , by:

$$\alpha ::= \nu x.\bar{n}\langle x \rangle @l \mid n(t) @l \mid \nu x_0.\langle x_0 \rangle \triangleright n_0, \dots, \nu x_i.\langle x_i \rangle \triangleright n_i \mid (t) \triangleleft l$$

$\nu x$  is a variable binder and the free and bound variables of  $\alpha$ , denoted by  $fv(\alpha)$  and  $bv(\alpha)$  respectively, are defined as expected. We write  $u \in \alpha$  if  $u$  belongs to the names or the free and bound variables of  $\alpha$ . Instead of  $\nu x_0.\langle x_0 \rangle \triangleright n_0, \dots, \nu x_i.\langle x_i \rangle \triangleright n_i$  we write  $\nu \tilde{x}.\langle \tilde{x} \rangle \triangleright \tilde{n}$  whenever  $\tilde{x} = x_0, \dots, x_i$  and  $\tilde{n} = n_0, \dots, n_i$  and we identify  $\nu x_0.\langle x_0 \rangle \triangleright n_0, \dots, \nu x_i.\langle x_i \rangle \triangleright n_i$  with any permutation of  $\nu x_0.\langle x_0 \rangle \triangleright n_0, \dots,$  and  $\nu x_i.\langle x_i \rangle \triangleright n_i$ .

Formally the semantics  $(\mathbf{N}, \{\longrightarrow, \xrightarrow{\alpha} \subseteq \mathbf{N} \times \mathbf{N} \mid \alpha \in \mathcal{A}\})$  is defined by extending the rules in Table 2 by the ones in Table 4. The rule (*out*) says that a ground term bound to a new variable  $x$  is output at name  $n$  at location  $l$  and dually (*in*) says that a term is input on name  $n$  at location  $l$ . Broadcast is taken care of by the rules (*brd*), (*syn*), and (*cls*). In (*brd*) a ground term is

<sup>6</sup> The semantics is tailored towards showing that our weak bisimulation is a congruence, a similar result will most likely not hold for a strong bisimulation.

|   |
|---|
| $(out) \frac{}{[\bar{n}\langle \hat{t} \rangle . p]_l \xrightarrow{\nu x . \bar{n}\langle x \rangle @ l} [p \parallel \{\hat{t}/x\}]_l} \quad x \notin fv(p) \quad (in) \frac{}{[n(x) . p]_l \xrightarrow{n(t) @ l} [p\{t/x\}]_l}$  |
| $(brd) \frac{}{[\langle \hat{t} \rangle . p]_l \parallel \{\tilde{n} \mapsto l\} \xrightarrow{\nu \tilde{x} . \langle \tilde{x} \rangle \triangleright \tilde{n}} [p]_l \parallel \prod_{k \in \tilde{n}} [\{\hat{t}/x_k\}]_k \parallel \{\tilde{n} \mapsto l\}} \quad \tilde{x} = (x_k)_{k \in \tilde{n}} \\ \tilde{x} \cap fv(p) = \emptyset$   |
| $(syn) \frac{E \xrightarrow{\nu \tilde{x} x . \langle \tilde{x} x \rangle \triangleright \tilde{n} l} E'}{E \parallel [(x) . p]_l \xrightarrow{\nu \tilde{x} x . \langle \tilde{x} x \rangle \triangleright \tilde{n} l} E' \parallel [p]_l} \quad (cls) \frac{E \xrightarrow{\nu \tilde{x} x . \langle \tilde{x} x \rangle \triangleright \tilde{n} l} E'}{E \xrightarrow{\nu \tilde{x} . \langle \tilde{x} \rangle \triangleright \tilde{n}} \nu x . E'}$ |
| $(rec) \frac{}{\prod_{k \in \tilde{n}} [(x) . p_k]_k \parallel \{\tilde{n} \mapsto l\} \xrightarrow{(t) @ l} \prod_{k \in \tilde{n}} [p_k\{t/x\}]_k \parallel \{\tilde{n} \mapsto l\}}$   |
| $(par) \frac{E \xrightarrow{\alpha} E'}{E \parallel F \xrightarrow{\alpha} E' \parallel F} \quad bv(\alpha) \cap fv(F) = \emptyset$   |
| $(new) \frac{E \xrightarrow{\alpha} E'}{\nu u . E \xrightarrow{\alpha} \nu u . E'} \quad u \notin \alpha \quad (str) \frac{E \equiv F \xrightarrow{\alpha} F' \equiv E'}{E \xrightarrow{\alpha} E'}$  |

**Table 4.** Transition Rules.

broadcasted to a set of locations  $\tilde{n}$  that all are connected to and hence within range of the broadcasting node  $l$ , the term is bound to a unique fresh variable in each receiving location. The rule *(syn)* allows a process to receive a broadcasted term as part of a broadcasting session if the process belongs to a location  $l$  within broadcast range. Rule *(cls)* closes a broadcast to one of the locations. The rule *(rec)* deals with reception of a broadcasted term from a location  $l$  in the environment. The remaining rules *(par)*, *(new)*, and *(str)* are standard.

As in [1] we introduce the notion of two terms  $s$  and  $t$  being equal in a frame  $\phi$ , denoted by  $s =_\phi t$ , and defined by:

**Definition 7.**  $s =_\phi t$  iff  $\phi \equiv \nu \tilde{n} . \{\tilde{t}/\tilde{x}\}$  and  $s\{\tilde{t}/\tilde{x}\} = t\{\tilde{t}/\tilde{x}\}$  with  $\tilde{n} \cap (fn(s) \cup fn(t)) = \emptyset$ .

**Definition 8.** Two frames  $\phi$  and  $\psi$  are static equivalent, denoted by  $\phi \sim_s \psi$ , if  $dom(\phi) = dom(\psi)$  and  $s =_\phi t$  iff  $s =_\psi t$  for all  $s$  and  $t$ .

We extend the notion of static equivalence to extended networks. Define the frame,  $\{E\}_l$ , at the free location  $l$  of  $E$  inductively by:  $\{P\}_l = \{\nu l . E\}_l = 0$ ,  $\{E \parallel F\}_l = \{E\}_l \parallel \{F\}_l$ ,  $\{\nu u . E\}_l = \nu u . \{E\}_l$  if  $l \neq u$ ,  $\{[e]_k\}_l = 0$  if  $l \neq k$ , and  $\{[e]_l\}_l = \{e\}$  where the frame,  $\{e\}$ , of  $e$  is defined inductively by:  $\{p\} = 0$ ,  $\{e \parallel f\} = \{e\} \parallel \{f\}$ ,  $\{\nu u . e\} = \nu u . \{e\}$ , and  $\{\{t/x\}\} = \{t/x\}$ . Notice that for  $E \in \mathbf{N}_c$  then  $\{E\}_l \equiv \nu \tilde{n} . \{\tilde{t}/\tilde{x}\}$  for some  $\tilde{t}$  and  $\tilde{x}$  where  $\tilde{n} \subseteq fn(\tilde{t})$  and  $fv(\tilde{t}) = \emptyset$ .

**Definition 9.** Two closed extended networks  $E$  and  $F$  are static equivalent, denoted by  $E \sim_s F$ , if  $\{E\}_l \sim_s \{F\}_l$  for all  $l$ .

Below we give a co-inductive characterization of  $\cong$ . We write  $E \xrightarrow{\nu\tilde{x}.\langle\tilde{x}\rangle\triangleright\tilde{n}} E'$  whenever there exists

$$E \Longrightarrow E_1 \xrightarrow{\nu\tilde{x}_1.\langle\tilde{x}_1\rangle\triangleright\tilde{n}_1} \dots \Longrightarrow E_{i-1} \xrightarrow{\nu\tilde{x}_i.\langle\tilde{x}_i\rangle\triangleright\tilde{n}_i} E_i \Longrightarrow E'$$

where  $\tilde{x} = \tilde{x}_1 \dots \tilde{x}_i$  and  $\tilde{n} = \tilde{n}_1 \dots \tilde{n}_i$ , otherwise we write  $E \xrightarrow{\alpha} E'$  whenever  $E \Longrightarrow \alpha \Longrightarrow E'$ . Also, for any  $\phi \equiv \nu\tilde{n}.\{\tilde{t}/\tilde{x}\}$  with  $fv(\tilde{t}) = \emptyset$  we write  $E \circ \phi$  for  $\nu\tilde{n}.E\{\tilde{t}/\tilde{x}\}$  assuming  $\tilde{n} \cap fn(E) = \emptyset$ .

**Definition 10.** A symmetric relation  $\mathcal{R}$  on  $\mathbf{N}_c$  is a weak bisimulation if  $E \mathcal{R} F$  implies  $E \sim_s F$  and

if  $E \longrightarrow E'$  then  $\exists F'. F \Longrightarrow F'$  and  $E' \mathcal{R} F'$

if  $E \xrightarrow{\nu x.\bar{n}(x)^{\otimes l}} E'$  then  $\exists F'. F \xrightarrow{\nu x.\bar{n}(x)^{\otimes l}} F'$  and  $E' \mathcal{R} F'$

if  $E \xrightarrow{\nu\tilde{x}.\langle\tilde{x}\rangle\triangleright\tilde{n}} E'$  then  $\exists F'. F \xrightarrow{\nu\tilde{x}.\langle\tilde{x}\rangle\triangleright\tilde{n}} F'$  and  $E' \mathcal{R} F'$

if  $E \xrightarrow{n(t)^{\otimes l}} E'$  and  $fv(t) \subseteq dom_l(E)$  then  $\exists F'. F \xrightarrow{n(t)^{\otimes l}} F'$  and  $E' \mathcal{R} F'$

if  $E \xrightarrow{(t)\triangleleft l} E'$  and  $fv(t) \subseteq dom_l(E)$  then  $\exists F'. F \xrightarrow{(t)\triangleleft l} F'$  and  $E' \circ \{E\}_l \mathcal{R} F' \circ \{F\}_l$

The largest weak bisimulation on  $\mathbf{N}_c$ ,  $\approx$ , is an equivalence relation.

The first three clauses in Definition 10 are standard. As in [1] the clauses for input require that free variables in the received term are already defined by the receiver. In our case this means that free variables received at a name  $n$  at  $l$  in  $E$  must also be defined at  $l$  in  $E$ . Likewise, free variables received by broadcast from  $l$  must be defined at  $l$  in  $E$  and these variables are substituted by the frame for location  $l$  at  $E$  preserving well-formedness.

**Theorem 3.**  $\approx$  is a congruence.

Weak bisimulation and weak barbed congruence coincides.

**Theorem 4.**  $\approx = \cong$ .

As usual we may define weak bisimulation up to  $\equiv$  and show that whenever  $\mathcal{R}$  is a weak bisimulation up to  $\equiv$  then  $\equiv \mathcal{R} \equiv$  is a weak bisimulation.

*Example 9.* Let  $\mathbf{P}_b$  be the set of extended processes with only broadcast prefixes. Then  $[e]_l \approx [e]_k$  for all  $e \in \mathbf{P}_b$  because  $\mathcal{R}$  is a weak bisimulation up to  $\equiv$  where

$$\mathcal{R} = \{(\nu\tilde{u}.\langle[e]_l \parallel E\rangle, \nu\tilde{u}.\langle[e]_k \parallel E\rangle) \mid E \in \mathbf{N}_c, l, k \notin \tilde{u}, \text{ and } e \in \mathbf{P}_b\}$$

*Example 10.* If  $l \notin fn(e)$  then  $\nu l.[e]_l \approx [e]_l$  for all  $e \in \mathbf{P}_b$  because  $\mathcal{R}$  is a weak bisimulation up to  $\equiv$  where

$$\begin{aligned} \mathcal{R} = \{ & (\nu\tilde{u}l.\langle[e]_l \parallel \{\tilde{n} \mapsto l\} \parallel \{l \mapsto \tilde{m}\} \parallel E, \nu\tilde{u}.\langle[e]_l \parallel E\rangle) \\ & \mid E \in \mathbf{N}_c, e \in \mathbf{P}_b, \text{ and } l \notin fn(e)\} \end{aligned}$$

*Example 11.*  $[\![\langle n \rangle . \langle m \rangle]\!]_l \approx [\![\langle m \rangle . \langle n \rangle]\!]_k$  because  $\mathcal{R}$  is a weak bisimulation up to  $\equiv$  where

$$\begin{aligned} \mathcal{R} = \{ & ([\![\langle n \rangle . \langle m \rangle]\!]_l \parallel \prod_{i \in I} [\langle n \rangle . \langle m \rangle]\!]_i \parallel \prod_{j \in J} [\langle m \rangle]\!]_j \parallel E, [\![\langle m \rangle . \langle n \rangle]\!]_k \parallel E), \\ & ([\![\langle n \rangle . \langle m \rangle]\!]_l \parallel E, [\![\langle m \rangle . \langle n \rangle]\!]_k \parallel \prod_{i \in I} [\langle m \rangle . \langle n \rangle]\!]_i \parallel \prod_{j \in J} [\langle n \rangle]\!]_j \parallel E) \\ & \mid E \in \mathbf{N}_c \text{ and } I \text{ and } J \text{ are finite index sets} \} \end{aligned}$$

*Example 12.* In order to prove  $E_{k,k'} \cong F$  from Example 8 it is sufficient to show

$$!\nu k. [r]_k \approx [r]_k \parallel [r]_{k'} \quad (3)$$

because  $\cong = \approx$  and because  $\approx$  is a congruence. Further, from Example 9 and 10 we infer that (3) follows from

$$[r]_k \parallel ! [r]_k \approx [r]_k \parallel [r]_k \quad (4)$$

because  $[r]_k \parallel ! [r]_k \approx ! [r]_k$ . The equivalence (4) in turn can be inferred from

$$[r]_k \parallel [r]_k \approx [r]_k \quad (5)$$

because then  $\mathcal{R} = \{(E \parallel ! [r]_k, F \parallel [r]_k) \mid E \approx F \parallel [r]_k\}$  is a weak bisimulation up to  $\equiv$ .<sup>7</sup> We leave the formal proof of (5) to the full version of this paper but clearly  $[r]_k \parallel [r]_k$  can do whatever  $[r]_k$  can, and as long as only one of the relay processes in  $[r]_k \parallel [r]_k$  at a time receives a request then  $[r]_k$  can do the same. Whenever both relay processes in  $[r]_k \parallel [r]_k$  receive the same request (and hence each may forward it) it may be necessary for  $[r]_k$  to forward the request also to itself in order to perform multiple forwarding of the same request.

## 5 Conclusion

In this paper we have discussed the presence of localities in observables for process calculi for mobile and wireless broadcasting systems. We have compared three kinds of barbs: the observability of *i*) output on a name at a given location, *ii*) broadcast of a name at some location, and *iii*) the broadcasting location respectively. For the three strong barbed congruences induced by each of these barbs we showed that they all coincide, however in the weak case the induced barbed congruence by the latter kind of barbs is strictly contained in the barbed congruences induced by the two former that coincide.

Our discussion has been carried out in the setting of a process calculus,  $bA\pi$ , that is a conservative extension of the Applied  $\pi$ -calculus.<sup>8</sup> We consider  $bA\pi$  a contribution of its own and to our knowledge it is the first calculus for mobile and wireless local broadcasting systems that allows for reasoning about an unbounded number of network nodes. Through examples we have demonstrated

<sup>7</sup> Observe that whenever  $[r]_k \xrightarrow{(t) \triangleleft l'} [r_0]_k$  for some  $t, l'$ , and  $r_0$  then  $[r_0]_k \approx \equiv [r_1]_k$  for some  $r_1$ .

<sup>8</sup> An Applied  $\pi$ -process  $p$  can be translated to  $[p]_l$  for some fixed  $l$  in  $bA\pi$ .

the applicability of  $bA\pi$  and given evidence to the weak reduction congruence,  $\cong$ , where the locality of a broadcasting node is not observable. Finally, we have proven the bisimulation equivalence,  $\approx$ , to be a *sound* and *complete* co-inductive characterization of  $\cong$ .

Several further developments of  $bA\pi$  lay forward. For instance it would be obvious to investigate automation of the bisimulation equivalence striving for a symbolic semantics along the lines of [4].

## References

1. M. Abadi and C. Fournet. Mobile vales, new names, and secure communication. In *Symposium on Principles of Programming Languages*, pages 104–115. ACM, 2001.
2. L. Cardelli and A.D. Gordon. Mobile ambients. In *FOSSACS*. Springer, 1998.
3. R. De Nicola, D. Gorla, and R. Pugliese. Basic observables for a calculus for global computing. *Information and Computation*, 205(10):1491–1525, 2007.
4. S. Delaune, S. Kremer, and M. Ryan. Symbolic bisimulation for the applied pi calculus. In *FSTTCS*, volume 4855 of *LNCS*. Springer, 2007.
5. J.C. Godskesen. A calculus for mobile ad hoc networks. In *COORDINATION*, volume 4467 of *LNCS*, pages 132–150. Springer, 2007.
6. J.C. Godskesen and S. Nanz. Mobility models and behavioural equivalence for wireless networks. In *COORDINATION*, volume 5521 of *LNCS*. Springer, 2009.
7. M. Merro. An observational theory for mobile ad hoc networks. *Electron. Notes Theor. Comput. Sci.*, 173:275–293, 2007.
8. M. Merro and E. Sibilio. A timed calculus for wireless systems. In *FSEN*, volume 5961 of *LNCS*. Springer, 2009.
9. N. Mezzetti and D. Sangiorgi. Towards a calculus for wireless systems. *Electr. Notes Theor. Comput. Sci.*, 158:331–353, 2006.
10. R. Milner. Functions as processes. In *Proceedings of Automata, Languages and Programming*, pages 167–180. Springer, 1990.
11. R. Milner. *Communicating and Mobile Systems: the  $\pi$ -Calculus*. Cambridge University Press, May 1999.
12. R. Milner and D. Sangiorgi. Barbed bisimulation. In *ICALP*, volume 623, pages 685–695. Springer, 1992.
13. S. Nanz and C. Hankin. A framework for security analysis of mobile wireless networks. *Theoretical Computer Science*, 367(1):203–227, 2006.
14. J. Riely and M. Hennessy. A typed language for distributed mobile processes (extended abstract). In *POPL '98*, pages 378–390, 1998.
15. D. Sangiorgi and D. Walker. *The  $\pi$ -calculus: A Theory of Mobile Processes*. Cambridge University Press, 2001.
16. A. Singh, C.R. Ramakrishnan, and S.A. Smolka. A process calculus for mobile ad hoc networks. In *COORDINATION*, volume 5052 of *LNCS*. Springer, 2008.