Available online at www.sciencedirect.com

ScienceDirect

ELSEVIER

Electronic Notes in Theoretical Computer Science 173 (2007) 275–293

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

An Observational Theory for Mobile Ad Hoc Networks

Massimo Merro[1]

Department of Computer Science
University of Verona
Verona, Italy

Abstract

We propose a process calculus to study the observational theory of *Mobile Ad Hoc Networks*. The operational semantics of our calculus is given both in terms of a *Reduction Semantics* and in terms of a *Labelled Transition Semantics*. We prove that the two semantics coincide. The labelled transition system is then used to derive the notions of simulation and bisimulation for ad hoc networks. As a main result, we prove that the (weak) *labelled bisimilarity* completely characterises (weak) reduction barbed congruence, a standard, branching-time, contextually-defined program equivalence. We then use our (bi)simulation proof methods to formally prove a number of non-trivial properties of ad hoc networks.

Keywords: Ad hoc networks, process calculi, structural operational semantics, bisimulation.

1 Introduction

Wireless technology has exploded in popularity in the last years. Its applications span 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.

Ad hoc networking is a new area in wireless communications that is attracting the attention of many researchers, for its potential to provide ubiquitous connectivity without the assistance of any fixed infrastructure. A *Mobile Ad Hoc Network* (MANET) is an autonomous system composed of both *stationary* and *mobile* devices communicating with each other via radio transceivers. Mobile devices are free to move randomly and organise themselves arbitrarily; thus, the network's wireless topology may change rapidly and *unpredictably*. Stationary devices cannot move i.e. their physical location does not vary with time. The network may operate in a standalone fashion, or may be connected to the larger Internet. MANETs can

[1] Email: Massimo.Merro@univr.it

doi:10.1016/j.entcs.2007.02.039

be used wherever a wired backbone is infeasible and/or economically inconvenient, for example, to provide communications during emergencies, special events (expos, concerts, etc.), or in hostile environments.

Wireless devices use radio frequency channels to *broadcast* messages to the other devices. However, this form of broadcast is quite different from the more conventional wired-based broadcast that we find in networks with Ethernet and that, from a semantic point of view, is well-understood [19,20,6]. First, in Ethernet-like systems broadcasting is global, i.e., the messages transmitted reach all nodes of the system. By contrast, in wireless system broadcasting is local, i.e., a transmission spans over a limited area, called *cell*, and therefore reaches only a -possibly empty- subset of the devices in the system. Actually, even the devices within a cell might not be reachable due to environmental conditions such as walls, obstacles, etc. Second, in wireless systems channels are *half-duplex*: on a given channel, a device can either transmit or receive, but cannot do both at the same time. Hence, an interference between two transmissions is only possibly detected by receivers located in the intersection of the cells of the two transmitters. *Interference* is thus a delicate aspect of wireless systems that is handled by means of specific protocols (e.g., CSMA/CA).

In mobile ad hoc networks there is a further catch: the set of nodes that lie within the cell of a node can change unpredictably due to node movement or node failure, thereby altering the set of nodes that can receive a transmitted message.

1.1 Contribution

We present the *Calculus of Mobile Ad Hoc Networks* (CMN), a process calculus to study the observational theory of mobile ad hoc networks. In CMN, a network is modelled as a collection of nodes (which represent devices), running in parallel, and using channels to broadcast messages. Channels can be either public or private to a set of nodes. We write $n[P]^{\mu}_{l,r}$ to denote a node with network address n, located at the physical location l, with transmission radius r, mobility tag μ, and executing the sequential process P. The location l and the transmission radius r define the *cell* over which a node can broadcast values using channels; by no means a node is capable to derive its current physical location l or its transmission radius r. The mobility tag μ serves to distinguish between mobile nodes and stationary nodes.

We assume the presence of appropriate protocols to avoid transmission collisions.

The operational semantics of our calculus is given both in terms of a *Reduction Semantics* and in terms of a *Labelled Transition Semantics*, in the SOS style of Plotkin [18]. We prove that the two semantics coincide. Our Labelled Transition System (LTS) captures all the possible interactions of a term with its environment without using any auxiliary discard relation. We then define an appropriate notion of *simulation* and hence of *bisimulation* for MANETs. The concepts of simulation and bisimulation are widely used in the literature for verification purposes: they represent the basis of many verification tools.

The main goal of the paper is to establish when two networks have the same *observable behaviour*, that is, they are indistinguishable in any context. In this paper, we focus on *reduction barbed congruence* [7], a slight variant of Milner and

Names:		$a, b, \ldots, k, l, m, n, \ldots \in \mathbf{N}$	
Networks:			
M, N	$::=$	$\mathbf{0}$	empty network
	$\mid$	$M_1 \mid M_2$	parallel composition
	$\mid$	$(\boldsymbol{\nu} c)M$	channel restriction
	$\mid$	$n[P]^{\mu}_{l,r}$	node (or device)
Processes:			
P, Q, R	$::=$	$\mathbf{0}$	inactive process
	$\mid$	$c(x).P$	input
	$\mid$	$\bar{c}\langle w \rangle.P$	output
	$\mid$	$[w_1 = w_2]P, Q$	matching
	$\mid$	$A\langle \tilde{v} \rangle$	recursion
Mobility tags:			
μ	$::=$	$\mathtt{m}$	mobile
	$\mid$	$\mathtt{s}$	stationary

Table 1
The Syntax

Sangiorgi's barbed congruence [13], a branching-time congruence that preserves the observables of the language. The definition of reduction barbed congruence is simple and intuitive. In practise, however, it is difficult to use: the quantification on all contexts is a heavy proof obligation. Simpler proof techniques are based on *labelled bisimilarities* [16,11]. As a main result, we prove that our (weak) labelled bisimilarity completely characterises reduction barbed congruence. We then use our observational theory to prove a number of non-trivial properties of MANETs.

Proofs are sketched or omitted. Full proofs can be found in [8].

2 The Calculus

In Table 1, we define the syntax of CMN in a two-level structure, a lower one for *processes* and an upper one for *networks*.

We use letters m and n for *nodes/devices*; c and d for *channels*; k and l for (physical) *locations*; x, y, z for *variables*. *Closed values* contain the previous entities except for channels and variables. *Values* include also variables. We use u and v for closed values and w for (open) values. We write $\tilde{a}$ to denote a tuple $a_1, \ldots, a_k$

of names.

Networks are collections of nodes (which represent devices), running in parallel, using channels to broadcast messages. The symbol $\mathbf{0}$ denotes the empty network. $M_1 \mid M_2$ represents the parallel composition of two networks. In $(\boldsymbol{\nu} c)M$ the channel c is private to the network M. Unlike other name-passing calculi, such as the π-calculus [12], the restriction operator $(\boldsymbol{\nu} c)M$ models only channel restriction but not channel creation. This is because the number of available channels in a wireless system is standardised by frequency throughout the world (13 for Europe, 11 for North America, and 14 for Japan).

Processes are sequential and live within the nodes. Process $\mathbf{0}$ denotes the inactive processes. The input process $c(x).P$ can receive any (closed) value v via channel c and continue as P, with v substituted for x. The output process $\overline{c}\langle v\rangle.P$ can send the (closed) value v via channel c and continue as P. Process $[v_1 = v_2]P, Q$ is the standard "if then else": it behaves as P if $v_1 = v_2$, and as Q otherwise. We write $A\langle\tilde{v}\rangle$ to denote a process defined via a (possibly recursive) definition $A(\tilde{x}) \stackrel{\text{def}}{=} P$, with $\mid \tilde{x} \mid = \mid \tilde{v} \mid$, where $\tilde{x}$ contains all channels and variables that appear free in P.

Each node has a location and a transmission radius. Nodes cannot be created or destroyed. We write $n[P]^{\mu}_{l,r}$ for a node named n, located at l, with transmission radius r, mobility tag μ, and executing process P. The node identifier n represents a logical location –the device network address. By contrast, l represents a physical location and, together with the radius r, is employed for deriving information about the network connectivity. The mobility tag μ can be $\mathtt{m}$ for *mobile nodes*, and $\mathtt{s}$ for *stationary nodes*, i.e. nodes that never change their physical location.

We do not indicate how locations should be specified; for instance, they could be given by means of a coordinate system. In the definition of the operational semantics, we assume the possibility of comparing locations so to determine whether a node lies or not within the transmission cell of another node. We do so by means of a function $\mathrm{d}(\cdot,\cdot)$ which takes two locations and returns their distance. In Section 5, we also assume some intuitive meta-operators on locations.

In the process $\overline{c}\langle w\rangle.P$ value w appears in *output position*; the function $\mathrm{op}(\cdot)$ returns the set of values appearing in output position in a process. In the process $c(x).P$ variable x is bound in P, giving rise to the standard notions of α-conversion and free and bound variables, denoted with $\mathrm{fv}(\cdot)$ and $\mathrm{bv}(\cdot)$, respectively. Similarly, in a network of the form $(\boldsymbol{\nu} c)M$ the channel name c is bound in M and the notions of α-conversion and free and bound channels, $\mathrm{fc}(\cdot)$ and $\mathrm{bc}(\cdot)$, are defined accordingly. We write $\{{}^{v}\!/\!_{x}\}P$ for the capture avoiding substitution of x for v in P. We will identify processes and networks up to α-conversion. More formally, we will view terms as representatives of their equivalence class with respect to $\equiv_\alpha$, and these representatives will always be chosen so that bound names are distinct from free names.

A (monadic) context $C[\cdot]$ is a network term with a hole, denoted by $[\cdot]$. Contexts are generated by the following grammar:

$$C[\cdot] \;::=\; [\cdot] \quad\Big|\quad [\cdot] \mid M \quad\Big|\quad M \mid [\cdot] \quad\Big|\quad (\boldsymbol{\nu} c)[\cdot] \ .$$

$A(\tilde{x}) \stackrel{\text{def}}{=} P \wedge \ \mid \tilde{x} \mid = \mid \tilde{v} \mid$ implies $n[A\langle \tilde{v} \rangle]^{\mu}_{l,r} \equiv n[\{{}^{\tilde{v}}\!/\!_{\tilde{x}}\}P]^{\mu}_{l,r}$	(Struct Proc)
$M \mid N \equiv N \mid M$	(Struct Par Comm)
$(M \mid N) \mid M' \equiv M \mid (N \mid M')$	(Struct Par Assoc)
$M \mid \mathbf{0} \equiv M$	(Struct Zero Par)
$(\boldsymbol{\nu} c)\mathbf{0} \equiv \mathbf{0}$	(Struct Zero Res)
$(\boldsymbol{\nu} c)(\boldsymbol{\nu} d)M \equiv (\boldsymbol{\nu} d)(\boldsymbol{\nu} c)M$	(Struct Res Res)
$c \notin \mathrm{fc}(M)$ implies $(\boldsymbol{\nu} c)(M \mid N) \equiv M \mid (\boldsymbol{\nu} c)N$	(Struct Res Par)
$[w = w]P, Q \equiv P$	(Struct Then)
$[w_1 = w_2]P, Q \equiv Q \quad$ if $w_1 \neq w_2$	(Struct Else)
$M \equiv M$	(Struct Refl)
$M \equiv N$ implies $N \equiv M$	(Struct Symm)
$M \equiv N \ \wedge \ N \equiv O$ implies $M \equiv O$	(Struct Trans)
$M \equiv N$ implies $M \mid M' \equiv N \mid M'$, for all M'	(Struct Cxt Par)
$M \equiv N$ implies $(\boldsymbol{\nu} c)M \equiv (\boldsymbol{\nu} c)N$, for all c	(Struct Cxt Res)

Table 2
Structural Congruence

We use a number of notational conventions. Parallel composition of networks has lower precedence with respect to restriction. $\prod_{i \in I} M_i$ means the parallel composition of all networks M_i, for $i \in I$. We write $(\boldsymbol{\nu} \tilde{c})M$ as an abbreviation for $(\boldsymbol{\nu} c_1) \ldots (\boldsymbol{\nu} c_k)M$. We write $\overline{c}\langle w \rangle$ for $\overline{c}\langle w \rangle.\mathbf{0}$, and $\mathbf{0}$ for $n[\mathbf{0}]^{\mu}_{l,r}$. Finally, we write $[w_1 = w_2]P$ for $[w_1 = w_2]P, \mathbf{0}$.

We assume that there are no free variables in a network (in contrast, there can be free channels). The absence of free variables is trivially maintained as the network evolves. Moreover, as node identifiers denote device network addresses we assume that in any network each node identifier is unique.

2.1 Reduction Semantics

The dynamics of the calculus is specified by the *reduction relation* over networks, $\rightarrowtriangle$, described in Table 3. As usual in process calculi, the *reduction semantics* relies on an auxiliary relation, called *structural congruence*, $\equiv$, defined in Table 2. Basically, structural congruence brings the participants of a potential interaction into contiguous positions.

Rule (R-Bcast) models the broadcast of a message v using a channel c. Communication is *one-to-many* and transmission proceeds even if there is no other process

$$(\text{R-Bcast})\ \frac{\forall i \in I.\ \mathrm{d}(l, l_i) \leq r}{n[\overline{c}\langle v\rangle.P]^{\mu}_{l,r} \mid \prod_{i\in I} n_i[c(x_i).P_i]^{\mu_i}_{l_i,r_i} \rightarrowtriangle n[P]^{\mu}_{l,r} \mid \prod_{i\in I} n_i[\{{}^{v}\!/\!_{x_i}\}P_i]^{\mu_i}_{l_i,r_i}}$$

$$(\text{R-Move})\ \frac{-}{n[P]^{\mathtt{m}}_{k,r} \rightarrowtriangle n[P]^{\mathtt{m}}_{l,r}} \qquad (\text{R-Par})\ \frac{M \rightarrowtriangle M'}{M \mid N \rightarrowtriangle M' \mid N}$$

$$(\text{R-Struct})\ \frac{M \equiv N \quad N \rightarrowtriangle N' \quad N' \equiv M'}{M \rightarrowtriangle M'} \qquad (\text{R-Res})\ \frac{M \rightarrowtriangle M'}{(\boldsymbol{\nu} c)M \rightarrowtriangle (\boldsymbol{\nu} c)M'}$$

Table 3
Reduction Semantics

listening for a message: transmission is a *non-blocking* action. Moreover, as with most process calculi, this communication is deemed to occur instantaneously. Note that when a transmission occurs, some receivers within the range of the transmitter might not receive the message. This may be due to several reasons such as the presence of obstacles or the asynchrony of nodes. In particular, when $I{=}\emptyset$ the rule models message loss. In terms of observation this corresponds to a local activity on the network which an observer is not party to. Movement is assumed to be an atomic action: while moving a node cannot do anything else. Rule (R-Move) models arbitrary and unpredictable movements of mobile nodes; notice that stationary nodes cannot move. The remaining rules are standard in process calculi.

The symbol $\rightarrowtriangle^*$ denotes the reflexive and transitive closure of $\rightarrowtriangle$.

2.2 Behavioural Semantics

In operational semantics two terms are deemed equivalent if they have the same observable behaviour in all possible contexts. So, the question is: What are the "right" observables in our calculus? As in CCS [11] and in π-calculus [12], we have both transmission and reception of messages. However, unlike those calculi, only the transmission of messages (over unrestricted channels) can be observed. In fact, in a broadcasting calculus an observer cannot see whether a given process actually receive a particular broadcasted value. In particular, if the node $n[\overline{c}\langle v\rangle.P]^{\mu}_{l,r}$ evolves into $n[P]^{\mu}_{l,r}$ we cannot be sure that some recipient received message v at channel c. On the other hand, if a node $n[c(x).P]^{\mu}_{l,r}$ evolves into $n[\{{}^{v}\!/\!_{x}\}P]^{\mu}_{l,r}$, then n can be sure that some node has transmitted message v on channel c: the network never invents messages!

So, in our calculus the notion of observability is represented by the transmission of messages that can be detected by a pervasive observer i.e. an observer that can listen anywhere, at any channel.

Definition 2.1 We write $M \downarrow_{c@k}$ if $M \equiv (\boldsymbol{\nu}\tilde{d})(n[\overline{c}\langle v\rangle.P]^{\mu}_{l,r} \mid M')$, with $c \notin \tilde{d}$ and $\mathrm{d}(l,k) \leq r$. We write $M \Downarrow_{c@k}$ if $M \rightarrowtriangle^* M' \downarrow_{c@k}$.

In the following, we use $\mathcal{R}$ to denote an arbitrary binary relation over networks.

$$\text{(Input)}\ \frac{-}{c(x).P \xrightarrow{cv} \{{}^{v}\!/\!_{x}\}P} \qquad\qquad \text{(Output)}\ \frac{-}{\overline{c}\langle v\rangle.P \xrightarrow{\overline{c}v} P}$$

$$\text{(Then)}\ \frac{P \xrightarrow{\eta} P'}{[v = v]P, Q \xrightarrow{\eta} P'} \qquad\qquad \text{(Else)}\ \frac{Q \xrightarrow{\eta} Q' \quad v_1 \neq v_2}{[v_1 = v_2]P, Q \xrightarrow{\eta} Q'}$$

$$\text{(Rec)}\ \frac{\{{}^{\tilde{v}}\!/\!_{\tilde{x}}\}P \xrightarrow{\eta} P' \quad A(\tilde{x}) \overset{\text{def}}{=} P}{A\langle\tilde{v}\rangle \xrightarrow{\eta} P'}$$

Table 4
Labelled Transition System - Processes

We write $\mathcal{R}^{=}$ to denote the symmetric closure of $\mathcal{R}$.

Definition 2.2 A relation $\mathcal{R}$ is *barb preserving* if $M \ \mathcal{R} \ N$ and $M \downarrow_{c@k}$ implies $N \Downarrow_{c@k}$.

Definition 2.3 A relation $\mathcal{R}$ is *reduction closed* if $M \ \mathcal{R} \ N$ and $M \rightarrowtriangle M'$ imply the existence of some N' such that $N \rightarrowtriangle^* N'$ and $M' \ \mathcal{R} \ N'$.

Definition 2.4 A relation $\mathcal{R}$ is *contextual* if $M \ \mathcal{R} \ N$ implies $\mathcal{C}[M] \ \mathcal{R} \ \mathcal{C}[N]$ for all contexts $\mathcal{C}[-]$.

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

Definition 2.5 Reduction barbed congruence, written $\cong$, is the largest symmetric relation over networks, which is reduction closed, barb preserving, and contextual.

3 A Labelled Transition Semantics

Reflecting the language syntax, the Labelled Transition System has two sets of rules: one for processes and one for networks.

Table 4 presents the LTS for processes. Transitions are of the form $P \xrightarrow{\eta} P'$, where η ranges over input and output actions. More precisely, cv and $\overline{c}v$ denote, respectively, input and output of a closed value v at channel c. The rules in Table 4 are self-explanatory.

Table 5 contains the LTS for networks. Transitions are of the form $M \xrightarrow{\lambda} M'$, where the grammar for λ is:

$$\lambda \ ::= \ c?v@l \ \mid \ c!v[l, r] \ \mid \ c!v@K \ \mid \ \tau \ .$$

Rule (Rcv) models the reception at l of message v via channel c. Rule (Snd) models the broadcast, with transmission radius r, of message v via channel c, from a node located at l. Rule (Bcast) models the propagation of broadcast. The requirement $\mathrm{d}(l, l') \leq r$ guarantees that only nodes within the transmission cell of the transmitter may hear the communication. Rule (Obs) models the fact that every action $c!v[l, r]$ can be detected (and hence *observed*) by any node located in the transmission cell

$$(\text{Rcv})\ \frac{P \xrightarrow{cv} P'}{n[P]^{\mu}_{l,r} \xrightarrow{c?v@l} n[P']^{\mu}_{l,r}} \qquad\qquad (\text{Snd})\ \frac{P \xrightarrow{\bar{c}v} P'}{n[P]^{c}_{l,r} \xrightarrow{c!v[l,r]} n[P']^{c}_{l,r}}$$

$$(\text{Bcast})\ \frac{M \xrightarrow{c!v[l,r]} M' \quad N \xrightarrow{c?v@l'} N' \quad \mathrm{d}(l,l') \leq r}{\begin{array}{c} M \mid N \xrightarrow{c!v[l,r]} M' \mid N' \\ N \mid M \xrightarrow{c!v[l,r]} N' \mid M' \end{array}}$$

$$(\text{Obs})\ \frac{M \xrightarrow{c!v[l,r]} M' \quad K{\subsetneq}\{k : \mathrm{d}(l,k){\leq}r\} \quad K{\neq}\emptyset}{M \xrightarrow{c!v@K} M'}$$

$$(\text{Lose})\ \frac{M \xrightarrow{c!v[l,r]} M'}{M \xrightarrow{\tau} M'} \qquad\qquad (\text{Move})\ \frac{-}{n[P]^{\mathtt{m}}_{k,r} \xrightarrow{\tau} n[P]^{\mathtt{m}}_{l,r}}$$

$$(\text{Par})\ \frac{M \xrightarrow{\lambda} M'}{\begin{array}{c} M \mid N \xrightarrow{\lambda} M' \mid N \\ N \mid M \xrightarrow{\lambda} N \mid M' \end{array}} \qquad\qquad (\text{Res})\ \frac{M \xrightarrow{\lambda} M' \quad c \notin \mathrm{fc}(\lambda)}{(\boldsymbol{\nu} c)M \xrightarrow{\lambda} (\boldsymbol{\nu} c)M'}$$

Table 5
Labelled Transition System - Networks

at l with radius r. The action $c!v@K$ represents the transmission of message v via channel c to a set of recipients whose locations are contained in K. This is an observable action: one can imagine a distributed observer listening on channel c and seated at any location of K. Rule (Lose) models both message loss and a local activity on the network which an observer is not party to. We use τ-actions, as usual in name-passing calculi, to denote non-observable actions, i.e. actions that are not detected by the observer. Rule (Move) models the migration of a mobile node from a location k to a new location l. Rule (Par) and (Res) are standard in name-passing calculi. Note that since we do not transmit channels there is no scope extrusion.

We end this section showing that the LTS-based semantics coincides with the reduction semantics given in the previous section in Table 3.

Theorem 3.1 (Harmony Theorem)

(i) *If* $M \xrightarrow{\tau} M'$ *then* $M \rightarrowtriangle M'$.

(ii) *If* $M \rightarrowtriangle M'$ *then* $M \xrightarrow{\tau}\equiv M'$.

4 Bi-simulation Proof Methods

In this section, we use our LTS to define an appropriate notion of simulation/bisimulation for ad hoc networks.

For commodity, we use the metavariable α to range over those actions that will be used in the definition of (bi)simulation. Formally,

$$\alpha \ ::= \ c?v@l \ \Big| \ c!v@K \ \Big| \ \tau \ .$$

Since we are interested in *weak behavioural equivalences*, that abstract over τ-actions, we introduce the notion of weak action. The definition is not completely standard:

- $\Rightarrow$ denotes the reflexive and transitive closure of $\xrightarrow{\tau}$;
- $\xRightarrow{c?v@l}$ denotes $\Rightarrow \xrightarrow{c?v@l} \Rightarrow$;
- $\xRightarrow{c!v@K}$ denotes $\Rightarrow \xrightarrow{c!v@K_1} \Rightarrow \dots \Rightarrow \xrightarrow{c!v@K_n} \Rightarrow$, for $\bigcup_{i=1}^{n} K_i = K$;
- $\xRightarrow{\hat{\alpha}}$ denotes $\Rightarrow$ if $\alpha = \tau$ and $\xRightarrow{\alpha}$ otherwise.

Notice that the definition of the weak observable action $\xRightarrow{c!v@K}$ may contain several (strong) observable actions of the form $\xrightarrow{c!v@K_i}$. This is because a distributed observer that receives in several computation steps an instance of message v at each location in K cannot assume that those messages belong to the same multicast send.

Definition 4.1 A binary relation $\mathcal{R}$ over networks is a *simulation* if $M \ \mathcal{R} \ N$ implies:

- If $M \xrightarrow{\alpha} M'$, $\alpha \neq c?v@l$, then there is N' such that $N \xRightarrow{\hat{\alpha}} N'$ and $M' \ \mathcal{R} \ N'$;
- If $M \xrightarrow{c?v@l} M'$ then there is N' such that:
  · either $N \xRightarrow{c?v@l} N'$ and $M' \ \mathcal{R} \ N'$
  · or $N \Rightarrow N'$ and $M' \ \mathcal{R} \ N'$.

We say that N *simulates* M if there is some simulation $\mathcal{R}$ such that $M \ \mathcal{R} \ N$. 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 $M \ \mathcal{R} \ N$.

Notice that, since reception of messages cannot be directly detected, the clause for message reception imposes weaker requirements, allowing to match input actions with τ-actions.

It is easy to show that our labelled bisimilarity is an equivalence relation. However, our bisimilarity enjoys a much more important property: the closure under contexts.

Lemma 4.2 ($\approx$ is contextual) *Let M and N be two networks such that $M \approx N$. Then,*

(i) *$M \mid O \approx N \mid O$, for all networks O;*
(ii) *$(\boldsymbol{\nu} c)M \approx (\boldsymbol{\nu} c)N$, for all channels c.*

Proof (Sketch) We only prove that $\approx$ is preserved by parallel composition. We demonstrate that the relation

$$\mathcal{S} \stackrel{\text{def}}{=} \{\big(M \mid O\,,\, N \mid O\big) \text{ for all } O \text{ such that } M \approx N\}$$

is a bisimulation. We do a case analysis on the transition $M \mid O \xrightarrow{\alpha} \hat{M}$. The interesting cases are when the transition is due to an interaction between M and O, i.e. when rule (Bcast) is used.

Let $M \mid O \xrightarrow{c!v@K} \hat{M}$ because $M \mid O \xrightarrow{c!v[l,r]} \hat{M}$ for some l and r, with $\mathrm{d}(l,k) \leq r$, for all $k \in K$ due to an application of rule (Bcast). There are two possibilities:

- $M \mid O \xrightarrow{c!v[l,r]} \hat{M}$ because $M \xrightarrow{c!v[l,r]} M'$ and $O \xrightarrow{c?v@l'} O'$, with $\mathrm{d}(l,l') \leq r$ and $\hat{M} = M' \mid O'$. In this case, by an application of rule (Obs) we have $M \xrightarrow{c!v@K'} M'$, with $K' = K \cup \{l'\}$. As $M \approx N$ there is N' such that $N \xRightarrow{c!v@K'} N'$ with $M' \approx N'$. By applying rule (Obs) backward there must be $K_1, \ldots, K_n$ such that $N \Rightarrow \xrightarrow{c!v@K_1} \ldots \xrightarrow{c!v@K_n} \Rightarrow N'$ with $\bigcup_{i=1}^{n} K_i = K'$ and $l' \in K_j$, for some $1 \leq j \leq n$. This implies that

$$N \Rightarrow \xrightarrow{c!v@K_1} \ldots \Rightarrow \xrightarrow{c!v[l_j,r_j]} \Rightarrow \ldots \xrightarrow{c!v@K_n} \Rightarrow N'$$

with $\mathrm{d}(l_j,k) \leq r_j$, for all $k \in K_j$. Hence by an application of rule (Bcast):

$$N \mid O \Rightarrow \xrightarrow{c!v@K_1} \ldots \Rightarrow \xrightarrow{c!v[l_j,r_j]} \Rightarrow \ldots \xrightarrow{c!v@K_n} \Rightarrow N' \mid O'\ .$$

Finally, by applying rule (Obs) we can turn the transition $\xrightarrow{c!v[l_j,r_j]}$ in $\xrightarrow{c!v@K_j}$. This implies $N \mid O \xRightarrow{c!v@K} N' \mid O'$ with $\big(M' \mid O'\,,\, N' \mid O'\big) \in \mathcal{S}$, as required.

- $M \mid O \xrightarrow{c!v[l,r]} \hat{M}$ because $M \xrightarrow{c?v@l'} M'$ and $O \xrightarrow{c!v[l,r]} O'$, with $\mathrm{d}(l,l') \leq r$ and $\hat{M} = M' \mid O'$. As $M \approx N$ there is N' such that:
  - · either $N \xRightarrow{c?v@l'} N'$, with $M' \approx N'$; in this case

$$N \mid O \Rightarrow \xrightarrow{c!v[l,r]} \Rightarrow N' \mid O'$$

  and, by rule (Obs), also $N \mid O \xRightarrow{c!v@K} N' \mid O'$, with $\big(M' \mid O'\,,\, N' \mid O'\big) \in \mathcal{S}$, as required.
  - · or $N \Rightarrow N'$, with $M' \approx N'$; in this case, by applying rule (Par) we obtain $N \mid O \Rightarrow \xrightarrow{c!v[l,r]} \Rightarrow N' \mid O'$ and, by rule (Obs) also $N \mid O \xRightarrow{c!v@K} N' \mid O'$, with $\big(M' \mid O'\,,\, N' \mid O'\big) \in \mathcal{S}$, as required.

Let $M \mid O \xrightarrow{\tau} \hat{M}$ because $M \mid O \xrightarrow{c!v[l,r]} \hat{M}$. We reason as in the previous case.

The remaining cases, when there is no interaction between M and O, are easy to deal with.

□

In the following lemma we point out a close relationship between the observation predicate $\downarrow_{c@k}$ and a specific action.

Lemma 4.3

(i) *If $M \xrightarrow{c!v@K} M'$ then $M \downarrow_{c@k}$, for all $k \in K$;*

(ii) *if $M \downarrow_{c@k}$ then there is a value v and a set of locations K, with $k \in K$, such that $M \xrightarrow{c!v@K} M'$.*

We can now prove that our bisimilarity is a proof method for reduction barbed congruence, i.e. that $\approx$ is contained in $\cong$.

Theorem 4.4 (Soundness) *Let M and N be two arbitrary networks such that $M \approx N$, then $M \cong N$.*

Proof We recall that $\cong$ is the least symmetric relation which is reduction closed, barb-preserving, and contextual. In fact, the bisimilarity is reduction closed (using Theorem 3.1), barb-preserving (by Lemma 4.3), and contextual (by Lemma 4.2). Thus, $\approx \subseteq \cong$. □

As a main result, we prove that the labelled bisimilarity is more than a proof technique. Actually, it represents a complete characterisation of reduction barbed congruence.

When proving the completeness result, i.e. that reduction barbed congruence is contained in the labelled bisimilarity, we implicitly use a standard property of reduction barbed congruence.

Proposition 4.5 *If $M \cong N$ then*

- *$M \Downarrow_{c@k}$ iff $N \Downarrow_{c@k}$*
- *$M \Rightarrow M'$ implies there is N' such that $N \Rightarrow N'$ and $M' \cong N'$.*

Lemma 4.6 (Completeness) *Reduction barbed congruence is contained in the bisimilarity.*

Proof (Sketch) We prove that the relation $\mathcal{R} = \{(M, N) \mid M \cong N\}$ is a bisimulation. The result will then follow by co-induction. In this sketch we only consider output actions.

- Suppose that $M \;\mathcal{R}\; N$ and $M \xrightarrow{c!v@K} M'$, with $K = \{k_1, \ldots, k_n\}$. As the action $c!v@K$ can only be generated by an application of rule (Obs), it follows that $M \xrightarrow{c!v[l,r]} M'$ for some l and r such that $\mathrm{d}(l, k) \leq r$, for all $k \in K$.

  Let us build up a context which mimics the effect of the action $c!v@K$, and also allows us to subsequently compare the residuals of the two systems under consideration. Our context has the form:

$$C[\cdot] \;\stackrel{\text{def}}{=}\; [\cdot] \mid \prod_{i=1}^{n} \big(m_i[c(x).[x = v]\overline{\mathsf{f}_i}\langle x\rangle]^{\mathsf{s}}_{k_i,r_i} \mid n_i[\mathsf{f}_i(x).\overline{\mathsf{ok}_i}\langle x\rangle]^{\mathsf{s}}_{k_i,r_i} \big)$$

with names m_i, n_i, for $1{\leq}i{\leq}n$, and channel names f_i and ok_i, for $1{\leq}i{\leq}n$, fresh. Intuitively, the existence of the barbs on the fresh channels f_i indicates that the action has not yet happened, whereas the presence of the barbs on channels ok_i, together with the absence of the barbs on f_i, ensures that the action has been performed.

As $\cong$ is preserved by network contexts, $M \cong N$ implies $C[M] \cong C[N]$. As $M \xrightarrow{c!v[l,r]} M'$, it follows that

$$C[M] \;\; \Rightarrow \;\; M' \mid \prod_{i=1}^{n} \big(m_i[\mathbf{0}]^{\mathsf{s}}_{k_i,r_i} \mid n_i[\overline{\mathsf{ok}_i}\langle v\rangle]^{\mathsf{s}}_{k_i,r_i}\big) \;\; = \;\; \hat{M}$$

with $\hat{M} \not\Downarrow_{\mathsf{f}_i@k_i}$ and $\hat{M} \Downarrow_{\mathsf{ok}_i@k_i}$, for $1{\leq}i{\leq}n$.

The reduction sequence above must be matched by a corresponding reduction sequence $C[N] \Rightarrow \hat{N}$ with $\hat{M} \cong \hat{N}$, $\hat{N} \not\Downarrow_{\mathsf{f}_i@k_i}$ and $\hat{N} \Downarrow_{\mathsf{ok}_i@k_i}$, for $1{\leq}i{\leq}n$.

The constrains on the barbs allow us to deduce the structure of the above reduction sequence. That is:

$$C[N] \;\; \Rightarrow \;\; N' \mid \prod_{i=1}^{n} \big(m_i[\mathbf{0}]^{\mathsf{s}}_{k_i,r_i} \mid n_i[\overline{\mathsf{ok}_i}\langle v\rangle]^{\mathsf{s}}_{k_i,r_i}\big) \;\; \cong \;\; \hat{N} \;\; .$$

This implies that $N \xRightarrow{c!v@L} N'$, with $K \subseteq L$. More precisely, the derivative N' might be reached performing several outputs of message v along the same channel c. However, as all nodes m_i are reached by a transmission along channel c coming from N, we can be sure that $K \subseteq L$. It is then easy to show that $N \xRightarrow{c!v@K} N'$ by considering in the composition of the weak action only on those outputs addressed to the locations in K, and turning the others in τ-actions using rule (Lose).

As $\hat{M} \cong \hat{N}$ and reduction barbed congruence is preserved by restriction, we have

$$(\boldsymbol{\nu}\tilde{\mathsf{f}}, \tilde{\mathsf{ok}})\hat{M} \cong (\boldsymbol{\nu}\tilde{\mathsf{f}}, \tilde{\mathsf{ok}})\hat{N} \;\; .$$

As channels f_i and ok_i, for $1{\leq}i{\leq}n$, are fresh we have

- $(\boldsymbol{\nu}\tilde{\mathsf{f}}, \tilde{\mathsf{ok}})\hat{M} \;\; \equiv \;\; M' \mid (\boldsymbol{\nu}\tilde{\mathsf{f}}, \tilde{\mathsf{ok}})\big(\prod_{i=1}^{n} m_i[\mathbf{0}]^{\mathsf{s}}_{k_i,r_i} \mid n_i[\overline{\mathsf{ok}_i}\langle v\rangle]^{\mathsf{s}}_{k_i,r_i}\big)$
- $(\boldsymbol{\nu}\tilde{\mathsf{f}}, \tilde{\mathsf{ok}})\hat{N} \;\; \equiv \;\; N' \mid (\boldsymbol{\nu}\tilde{\mathsf{f}}, \tilde{\mathsf{ok}})\big(\prod_{i=1}^{n} m_i[\mathbf{0}]^{\mathsf{s}}_{k_i,r_i} \mid n_i[\overline{\mathsf{ok}_i}\langle v\rangle]^{\mathsf{s}}_{k_i,r_i}\big)$.

Using our labelled bisimilarity and Theorem 4.4 is easy to prove that

$$(\boldsymbol{\nu}\tilde{\mathsf{f}}, \tilde{\mathsf{ok}})\big(\prod_{i=1}^{n} m_i[\mathbf{0}]^{\mathsf{s}}_{k_i,r_i} \mid n_i[\overline{\mathsf{ok}_i}\langle v\rangle]^{\mathsf{s}}_{k_i,r_i}\big) \;\; \cong \;\; \mathbf{0} \;\; .$$

As a consequence, it follows that $M' \cong N'$, as required.

□

An easy consequence of Theorem 4.4 and Lemma 4.6 is the following.

Theorem 4.7 (Characterisation) *Bisimilarity and reduction barbed congruence coincide.*

5 Properties and examples

In this section, we prove a number of properties using our observational theory.

We start proving an interesting feature of mobile nodes.

Theorem 5.1 (Ubiquity of mobile nodes) *For any process P, physical locations k and l, and transmission radius r, it holds that*

$$n[P]^{\mathtt{m}}_{k,r} \;\approx\; n[P]^{\mathtt{m}}_{l,r} \;.$$

Proof We show that the relation

$$\mathcal{S} \overset{\mathrm{def}}{=} \{\big(\, n[P]^{\mathtt{m}}_{k,r},\, n[P]^{\mathtt{m}}_{l,r}\big) : \forall\, k, l\; \forall P\}^{=} \cup \mathcal{I}$$

is a bisimulation, where $\mathcal{I}$ is the identity relation. □

The next result shows that silent nodes cannot be detected (or observed). A node is said silent if it never transmit messages.

Theorem 5.2 (Silent nodes cannot be observed) *If process P does not contain output constructs, then*

$$n[P]^{\mu}_{l,r} \;\approx\; \mathbf{0}$$

for any l and r.

Proof It follows from our definition of bisimilarity in which it is possible to match both τ-actions and input actions with weak τ-actions. We recall that $\Rightarrow$ is the *reflexive* and transitive closure of $\xrightarrow{\tau}$. □

Now, we show how syntactically different infinite output sequences may be semantically indistinguishable, because of message loss.

Theorem 5.3 (Mixing up infinite output sequences)
Let $\mathrm{ALT}(a,b) \overset{\mathrm{def}}{=} \overline{c}\langle a\rangle.\overline{c}\langle b\rangle.\mathrm{ALT}\langle a,b\rangle$. *Then, for any l, n, r, u, and v it holds that:*

(i) $n[\,\mathrm{ALT}\langle u,v\rangle]^{\mathtt{s}}_{l,r} \;\approx\; n[\,\mathrm{ALT}\langle v,u\rangle]^{\mathtt{s}}_{l,r}$

(ii) $n[\,\mathrm{ALT}\langle u,v\rangle]^{\mathtt{m}}_{k,r} \;\approx\; n[\,\mathrm{ALT}\langle v,u\rangle]^{\mathtt{m}}_{l,r}$.

Proof We only prove the second statement. We show that the relation

$$\mathcal{R} \overset{\mathrm{def}}{=} \{\big(n[\,\mathrm{ALT}\langle u,v\rangle]^{\mathtt{m}}_{k,r}\,,\, n[\,\mathrm{ALT}\langle v,u\rangle]^{\mathtt{m}}_{l,r}\big) :\ \text{for all } k,l\}^{=} \cup \mathcal{I}$$

where $\mathcal{I}$ is the identity relation, is a bisimulation up to $\equiv$. □

This result can be generalised replacing u and v with an arbitrary finite set $V = \{v_1, \ldots, v_n\}$ of messages. More generally, if two nodes contain only an infinite sequence of output constructs transmitting values belonging to some finite set V, such that for each $v \in V$ the output $\overline{c}\langle v\rangle$ appears an infinite number of times, then the two nodes are equivalent.

In the next result, we show that devices transmitting messages "ad infinitum" may obfuscate the transmission activity of nodes which are transmitting the same messages within the same transmission cell. We recall that the function $\mathrm{fc}(\cdot)$ returns the set of free channels contained in one or more processes, while $\mathrm{op}(\cdot)$ returns the set of values appearing in output position in one or more processes.

Theorem 5.4 (Obfuscating message transmission) *Let P and Q be two processes such that $\mathrm{fc}(P,Q) \subseteq \{c\}$, for some channel c, and $\mathrm{op}(P,Q) \subseteq \{u,v\}$, for some values u and v. Let $\mathrm{ALT}(a,b) \stackrel{\mathrm{def}}{=} \overline{c}\langle a\rangle.\overline{c}\langle b\rangle.\mathrm{ALT}\langle a,b\rangle$. Then,*

(i) $n[P]^{\mathtt{s}}_{l,r} \;\mid\; m[\,\mathrm{ALT}\langle u,v\rangle]^{\mathtt{s}}_{l,r} \;\approx\; n[Q]^{\mathtt{s}}_{l,r} \;\mid\; m[\,\mathrm{ALT}\langle u,v\rangle]^{\mathtt{s}}_{l,r}$

(ii) $n[P]^{\mathtt{m}}_{k,r} \;\mid\; m[\,\mathrm{ALT}\langle u,v\rangle]^{\mathtt{m}}_{l,r} \;\approx\; n[Q]^{\mathtt{m}}_{k',r} \;\mid\; m[\,\mathrm{ALT}\langle u,v\rangle]^{\mathtt{m}}_{l',r}$.

Proof We only prove the first statement. By transitivity of $\approx$, it suffices to prove that

$$n[P]^{\mathtt{s}}_{l,r} \;\mid\; m[\,\mathrm{ALT}\langle u,v\rangle]^{\mathtt{s}}_{l,r} \;\approx\; m[\,\mathrm{ALT}\langle u,v\rangle]^{\mathtt{s}}_{l,r}$$

for all l and r, and for all P such that $\mathrm{fc}(P) \subseteq \{c\}$ and $\mathrm{op}(P) \subseteq \{u,v\}$. At this purpose, we show that the binary relation

$$\{\, \big(n[P]^{\mathtt{s}}_{l,r} \mid m[\,\mathrm{ALT}\langle u,v\rangle]^{\mathtt{s}}_{l,r}\,,\; m[\,\mathrm{ALT}\langle u,v\rangle]^{\mathtt{s}}_{l,r}\big) \,:\, {\scriptstyle \forall P.\ \mathrm{fc}(P)\subseteq\{c\} \wedge \mathrm{op}(P)\subseteq\{u,v\}} \,\}^{=}$$

$$\bigcup$$

$$\{\big(n[P]^{\mathtt{s}}_{l,r} \mid m[\overline{c}\langle v\rangle.\,\mathrm{ALT}\langle u,v\rangle]^{\mathtt{s}}_{l,r}, m[\overline{c}\langle v\rangle.\,\mathrm{ALT}\langle u,v\rangle]^{\mathtt{s}}_{l,r}\big) : {\scriptstyle \forall P.\,\mathrm{fc}(P)\subseteq\{c\} \wedge \mathrm{op}(P)\subseteq\{u,v\}}\}^{=}$$

is a bisimulation. □

Also this result can be generalised taking an arbitrary finite set V of messages.

The next results are about *range repeaters* (or range extender), and make particularly sense for stationary nodes, like access points. In general, a repeater simply regenerates a network signal in order to extend the range of the existing network infrastructure. In a wireless networks a range repeater does not physically connect by wire to any part of the network. Instead, it receives radio signals from an access point, end user device, or another repeater and retransmits the frames. This makes it possible for a repeater located in between an access point and a distant stationary user to act as a relay for frames travelling back and forth between the user and the access point. In this manner, using a range repeater, a distant user can get connected to the network.

In our calculus, a range repeater can be modelled as a node $\mathrm{rr}[c \hookrightarrow c]^{\mathtt{s}}_{l,r}$, where the process $c \hookrightarrow c$ is a forwarder process whose general recursive definition is

$$a \hookrightarrow b \;\stackrel{\mathrm{def}}{=}\; a(x).\overline{b}\langle x\rangle.a \hookrightarrow b$$

This process receives values at channel a and retransmits them on channel b; in $c \hookrightarrow c$ the same channel c is used for reception and transmission. We will use the definition of forwarder process in several examples.

Now, suppose we want to extend the range of an access point $n[P]^{\mathsf{s}}_{k,r}$. In particular, suppose we want to cover the cell located at l with radius r'. In this case, if $\mathrm{d}(k,l) \leq r$ and $\mathrm{d}(k,l) \leq r'$ we could add a range repeater at l that simply repeats the signal back and forth with transmission radius r'. In such a scenario, if node n is *single-channel*, i.e. it uses only one channel, then the introduction of the range repeater allows us to simulate the presence of the access point n at l with transmission radius r', i.e. $n[P]^{\mathsf{s}}_{l,r'}$.

Theorem 5.5 (Range repeaters) *Let P be a process such that $\mathrm{fc}(P) \subseteq \{c\}$, for some channel c. Let k, l be physical locations, and r, r' be transmission radii such that $\mathrm{d}(k,l) \leq r$ and $\mathrm{d}(k,l) \leq r'$. Then, the system*

$$n[P]^{\mathsf{s}}_{k,r} \;\big|\; \mathrm{rr}[c \hookrightarrow c]^{\mathsf{s}}_{l,r'}$$

simulates the node $n[P]^{\mathsf{s}}_{l,r'}$.

Proof We prove that the relation

$$\{\big(n[P]^{\mathsf{s}}_{l,r'}\,,\; n[P]^{\mathsf{s}}_{k,r} \,\big|\, \mathrm{rr}[c \hookrightarrow c]^{\mathsf{s}}_{l,r'}\big) : \forall k,l.\ \mathrm{d}(k,l){\leq}r \,\wedge\, \mathrm{d}(k,l){\leq}r',\ \forall P.\ \mathrm{fc}(P){\subseteq}\{c\}\}$$

is a simulation. □

A well-known downside of range repeaters, though, is that they reduce the throughput of the network. A range repeater must receive and retransmit each frame on the same radio frequency channel, which effectively doubles the number of frames that are sent. In particular, accordingly with the protocol CSMA/CA, whenever the range repeater transmits on channel c the node n must remain silent to avoid collisions. A way to avoid this inconvenient could be that of using more sophisticated range repeaters working on two different channels: for example, channel c for communicating with the access point n, and a different channel, say d, to interact with the local stationary users.

Theorem 5.6 (Range repeaters with two channels) *Let P be a process such that $\mathrm{fc}(P) \subseteq \{c\}$, for some channel c. Let k, l be physical locations, and r, s be transmission radii, such that $\mathrm{d}(k,l) \leq r$ and $\mathrm{d}(k,l) \leq r'$. Then, for any channel d, the system*

$$n[P]^{\mathsf{s}}_{k,r} \;\big|\; \mathrm{out}[c \hookrightarrow d]^{\mathsf{s}}_{l,r'} \;\big|\; \mathrm{in}[d \hookrightarrow c]^{\mathsf{s}}_{l,r'}$$

simulates the node $n[\{{}^{d}\!/\!_{c}\}P]^{\mathsf{s}}_{l,r'}$.

Proof We prove that the relation

$$\begin{aligned}\mathcal{S} \;\stackrel{\mathrm{def}}{=}\; \{\Big(& n[\{{}^{d}\!/\!_{c}\}P]^{\mathsf{s}}_{l,r'}\,,\; \big(n[P]^{\mathsf{s}}_{k,r} \;\big|\; \mathrm{out}[c \hookrightarrow d]^{\mathsf{s}}_{l,r'} \;\big|\; \mathrm{in}[d \hookrightarrow c]^{\mathsf{s}}_{l,r'}\big)\Big) : \\ & \forall\, k,l.\ \mathrm{d}(k,l){\leq}r \,\wedge\, \mathrm{d}(k,l){\leq}r' \\ & \forall\, P.\ \mathrm{fc}(P) \subseteq \{c\} \\ \}& \end{aligned}$$

is a simulation. □

As already pointed out, the previous results on range repeaters make particular sense when dealing with stationary nodes. In fact, when dealing with mobile nodes those devices are basically superfluous, as exemplified below.

Theorem 5.7 *Let k, l be physical locations and r, r' be transmission radii such that $r \geq r'$. Then,*

$$n[P]^{\mathtt{m}}_{k,r} \textit{ simulates } n[P]^{\mathtt{m}}_{l,r'} \quad .$$

Proof We show that the relation

$$\mathcal{S} \stackrel{\text{def}}{=} \{\big(n[P]^{\mathtt{m}}_{l,r'} \, , \, n[P]^{\mathtt{m}}_{k,r}\big) : \forall k, l \; \forall P\,\}$$

is a simulation. □

Finally, we provide a result concerning with energy consumption. It is well-know [23] that the power p_k required by a node located at k to correctly transmit data to a node located at l must satisfy the inequality $\frac{p_k}{\mathrm{d}(k,l)^\alpha} \geq \beta$, where $\alpha \geq 2$ is the *distance-power gradient* and $\beta \geq 1$ is the *transmission quality* parameter. [2] While the value of β is usually set to 1, the value of α depends on environmental conditions. In the ideal case, we have $\alpha = 2$; however α is typically 4 in realistic situations. For instance, for $r = 10$ the power p_k of the transmitter must be at least 10000.

However, if we introduce a repeater node between transmitter and receiver, say in the middle, we can drastically reduce the whole transmission power. More precisely, to cover the distance of 5 is enough a transmission power of 625. Thus, the transmission power we need for both the transmitter and the repeater is 1250 instead of 10000!

The following result shows that the introduction of a repeater between a first (stationary) node located at some l_1, and a second (stationary) node located at some l_2, using a private channel to propagate the signal, does not change the behaviour of the original system. Notice that for $\mathrm{d}(l_1, l_2) = r$, we write $l_1{+}r/2$ to denote the location placed in the middle, between l_1 and l_2.

Theorem 5.8 (Saving antenna power) *Let P be a process such that $\mathrm{fc}(P) = \{d\}$, for some channel d. Let l_1, l_2 be physical locations, and r_1, r_2 be transmission radii such that $\mathrm{d}(l_1, l_2) = r$, $r \leq r_1$, and $r \leq r_2$. Then, the system*

$$(\boldsymbol{\nu} d)\big(m[P]^{\mathtt{s}}_{l_1,r/2} \;\big|\; \mathrm{rr}\,[d \hookrightarrow d]^{\mathtt{s}}_{l_1+r/2,r/2} \;\big|\; n[Q]^{\mathtt{s}}_{l_2,r_2}\big)$$

simulates the system

$$(\boldsymbol{\nu} d)\big(m[P]^{\mathtt{s}}_{l_1,r_1} \;\big|\; n[Q]^{\mathtt{s}}_{l_2,r_2}\big) \quad .$$

[2] This inequality holds for free-space environments with non-obstructed line of sight, and it does not consider the possible occurrence of reflections, scattering, and diffraction caused by buildings, terrain, and so on. Nevertheless, it is widely accepted in the ad hoc network community.

Proof The two systems basically differ for the presence of the range repeater operating on the private channel d. Formally, we prove that the relation

$$\begin{aligned}
\{ & \Big((\boldsymbol{\nu} d)(m[P]^{\mathsf{s}}_{l_1,r_1} \,|\, n[Q]^{\mathsf{s}}_{l_2,r_2}) \,,\, (\boldsymbol{\nu} d)(m[P]^{\mathsf{s}}_{l_1,r/2} \,|\, \mathrm{rr}\,[d \hookrightarrow d]^{\mathsf{s}}_{l_1+r/2,r/2} \,|\, n[Q]^{\mathsf{s}}_{l_2,r_2}) \Big) : \\
& \quad \forall Q\, \forall P.\ \ \mathrm{fc}(P)=\{d\} \\
\} &
\end{aligned}$$

is a simulation. □

6 Related and Future Work

Broadcast for Ethernet-like communications has been first analysed by Prasad [19,20,15] in his *Calculus of Broadcasting Systems* (CBS), in which all processes receive a broadcast message at once. In [21] the same author proposed a LTS and a (both strong and weak) labelled bisimilarity relying on the notion of "discard relation", a special transition that any process can perform to discard a potential message. Technically speaking, the discard relation is a mechanism to fit the semantics of broadcast with that of parallel composition.

Hennessy and Rathke [6] proved that the above (weak) bisimilarity, renamed *noisy bisimilarity*, coincides with barbed congruence. Modulo the presence of the discard relation, our bisimilarity is very close to noisy bisimilarity.

The $b\pi$-calculus [2] of Ene and Muntean equips the π-calculus with a broadcast paradigm such that only nodes listening on the right channel can receive a broadcast. While this seems to come closer to a notion of local broadcast, it remains complicated to change a once established connectivity. The authors proposed an LTS (relying on the discard relation) and a labelled bisimilarity which is proved to coincide with barbed equivalence. They also proved that the closure under substitution of their labelled bisimilarity corresponds to the barbed congruence.

Nanz and Hankin [14] have introduced a calculus for Mobile Wireless Networks (CBS#) where the recipients of a transmission are determined using a graph representation of node localities. While this approach is more flexible, ours (based on location and radius that define transmission cells and distance) allows a more compact representation of connectivity. The authors proposed a LTS which is very close to that of [21,6] and again relies on the discard relation. This LTS is then used to define a behavioural equivalence, called *mediated equivalence* that identifies processes only with respect to their capability to store items. The final goal of Nanz and Hankin is to use their calculus as the basis of a framework for specification and security analysis of communication protocols for MANETs.

Prasad's more recent calculus of Mobile Broadcasting Systems, (MBS) [22] aims at providing a communication model which implements the "globally asynchronous, locally synchronous" communication mechanism which is proper of wireless communication communication systems. Channels are employed as sealed rooms, preventing a message sent within a room to being captured by processes in other rooms.

Singh, Ramakrishnan, and Smolka [24] have proposed the ω-calculus, a conservative extension of the π-calculus specifically tailored for modelling MANETs' protocols. The 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 latter is modelled annotating processes with the set of group names to which the process belongs. The authors have proposed a labelled transition semantics that, unlike the previous ones, does not use the discard relation but instead contains a rule, similar to our (Lose), to model the non-blocking nature of multicast send. A bisimulation in "open" style is provided. The ω-calculus is then used for developing a model of the AODV protocol [17], a routing protocol for MANETs.

Finally, notice that all the previous calculi abstract from interferences. Mezzetti and Sangiorgi [9] have instead proposed a lower level calculus in which a node can detect interferences when located in the intersection of the transmission range of two different nodes. While our syntax is inspired by that of [9], the reduction semantics and the corresponding LTS is quite different; this is because in our model we assume the absence of interferences.

6.1 Future Work

A number of developments are possible. For instance, we could enrich the calculus with operators to model the concept of store as in [14]. We could try to extend the behavioural theory to deal with node failure. At this regards, the developments in [3,4] for wired networks could be a good starting point. Moreover, wireless systems have also features of *synchrony* that remind us of synchronous languages (e.g. Esterel [1], Statecharts [5], SCCS [10]). Indeed, in a single time unit of a wireless system multiple events can happen. It is our intention to investigate these aspects taking inspiration from [22]. Finally, as pointed out in [14], security is, of course, another important issue in MANETs that we would like to investigate.

Acknowledgements Many thanks to Davide Sangiorgi for insightful comments on a early draft. I also thank Davide Quaglia for useful discussions on MANETs.

References

[1] G. Berry and G. Gonthier. The esterel synchronous programming language: Design, semantics, implementation. *Science of Computer Programming*, 19(2):87–152, 1992.

[2] C. Ene and T. Muntean. A Broadcast based Calculus for Communicating Systems. In *IPDPS*, page 149, 2001.

[3] A. Francalanza and M. Hennessy. A theory of system behaviour in the presence of node and link failures. In *CONCUR*, volume 3653 of *Lecture Notes in Computer Science*. Springer, 2005.

[4] A. Francalanza and M. Hennessy. A theory for observational fault tolerance. In *FoSSaCS*, volume 3921 of *Lecture Notes in Computer Science*, pages 16–31. Springer, 2006.

[5] D. Harel. Statecharts: A visual formulation for complex systems. *Science of Computer Programming*, 8(3):231–274, 1987.

[6] M. Hennessy and J. Rathke. Bisimulations for a Calculus of Broadcasting Systems. *Theoretical Computer Science*, 200:225–260, 1998.

[7] K. Honda and N. Yoshida. On reduction-based process semantics. *Theoretical Computer Science*, 152(2):437–486, 1995.

[8] M. Merro. An Observational Theory for Mobile Ad Hoc Networks. Technical Report 44/2006, Dipartimento di Informatica – Università degli studi di Verona, Italy, December 2006. Available at http://www.di.univr.it/report.

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

[10] R. Milner. Calculi for synchrony and asynchrony. *Theoretical Computer Science*, 25:267–310, 1983.

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

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

[13] R. Milner and D. Sangiorgi. Barbed bisimulation. In *ICALP*, volume 623 of *LNCS*, pages 685–695. Springer Verlag, 1992.

[14] S. Nanz and C. Hankin. A Framework for Security Analysis of Mobile Wireless Networks. *Theoretical Computer Science*, 2006. To appear.

[15] K. Ostrovsky, K. V. S. Prasad, and W. Taha. Towards a primitive higher order calculus of broadcasting systems. In *PPDP*, pages 2–13. ACM, 2002.

[16] D.M. Park. Concurrency on automata and infinite sequences. In P. Deussen, editor, *Conf. on Theoretical Computer Science*, volume 104 of *LNCS*. Springer Verlag, 1981.

[17] C.E. Perkins and E.M. Belding-Royer. Ad-hoc on-demand distance vector routing. In *2nd Workshop on Mobile Computing Systems and Applications (WMCSA '99)*, pages 90–100. IEEE Computer Society, 1999.

[18] G.D. Plotkin. A structural approach to operational semantics. Technical Report DAIMI-FN-19, Computer Science Department, Aarhus University, 1981.

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

[20] K. V. S. Prasad. Broadcasting in Time. In *COORDINATION*, volume 1061. LNCS, 1996.

[21] K.V.S. Prasad. A calculus of value broadcasts. In *PARLE: Parallel Architectures and Languages Europe*. LNCS, 1993.

[22] K.V.S. Prasad. A prospectus for mobile broadcasting systems. In *Proc. of the Workshop on Algebraic Process Calculi: The First Twenty Five Years and Beyond, (PA'05)*. BRICS Press, 2005.

[23] T. Rappaport. *Wireless Communications: Principles and Practice*. Monographs in Computer Science. 2nd Ed. Prentice Hall, 2002.

[24] A. Singh, C. R. Ramakrishnan, and S. A. Smolka. A Process Calculus for Mobile Ad Hoc Networks, 2006. Available at http://www.lmc.cs.sunysb.edu/~cram/Papers/SRS_OmegaCalc2006/.