Information and Computation 207 (2009) 194–208

Contents lists available at ScienceDirect

Information and Computation

journal homepage: www.elsevier.com/locate/ic

An Observational Theory for Mobile Ad Hoc Networks (full version)☆

Massimo Merro

Department of Computer Science, University of Verona, Italy

ARTICLE INFO

Article history:
Received 26 February 2007
Revised 30 August 2007
Available online 6 December 2008

Keywords:
Ad hoc network
Process calculus
Labelled Transition Semantics
Bisimulation

ABSTRACT

We propose a process calculus to study the behavioural 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 (weak) simulation and bisimulation for ad hoc networks. The *labelled bisimilarity* completely characterises reduction barbed congruence, a standard branching-time and contextually-defined program equivalence. We then use our (bi)simulation proof method to formally prove a number of non-trivial properties of ad hoc networks.

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. Ad hoc networks may operate in a standalone fashion, or may be connected to the larger Internet. They can 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 [20,21,7]. In Ethernet-like systems broadcasting has a *logical scope*, i.e., broadcast messages reach all devices belonging to some logically defined network. By contrast, in wireless systems broadcasting has a *physical scope*; this is because a radio transmission spans over a limited area, called transmission *cell*, and reaches only a—possibly empty—subset of the devices in the network. Actually, even the devices within the range of the transmitter might not receive the broadcast message due to environmental conditions such as walls, temporary obstacles, etc.

☆ This paper is a full version of the MFPS XXIII conference paper: M. Merro, An Observational Theory for Mobile Ad Hoc Networks, Electronic Notes in Theoretical Computer Science 173, Elsevier, 2007, pp. 275–293.

E-mail adress: massimo.merro@univr.it (M. Merro).

0890-5401/$ - see front matter © 2009 Published by Elsevier Inc.
doi:10.1016/j.ic.2007.11.010

In wireless networks 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., IEEE 802.11 CSMA/CA).

We propose a value-passing process calculus to model Mobile Ad Hoc Networks. Our calculus is called *Calculus of Mobile Ad Hoc Networks* (CMN). In CMN, an ad hoc 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. To keep focus on the peculiarities of wireless networks, channels in CMN are in CCS style [12]: they cannot be used to transmit channel names. The theory developed in this article can be generalised to a name-passing variant of CMN. We assume the presence of appropriate protocols to avoid transmission collisions.

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 which models the behaviour of the device. The location l and the transmission radius r define the *cell* over which a node can broadcast values using channels; a node is not able to derive its current physical location l (it does not support a GPS) or its transmission radius r. The mobility tag μ serves to distinguish between mobile nodes and stationary nodes.

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 propose an adequate behavioural theory to formally prove properties of ad hoc networks. To give an idea of what kind of properties we have in mind we just sketch here a couple of them. More properties with full details can be found in Section 6.

Ubiquity of mobile nodes. Node mobility is unpredictable and it cannot be directly observed by the environment. This means that we cannot distinguish two mobile nodes that differ only for their physical current location. Formally, for any process P, physical locations k and l, and transmission radius r, it holds that

$$n[P]^{\mathtt{m}}_{k,r} \text{ is bisimilar to } n[P]^{\mathtt{m}}_{l,r}$$

where the tag $\mathtt{m}$ denotes mobile nodes. Even more, a mobile node with transmission radius r can always simulate a mobile node with the same code but with a smaller transmission radius r'. Formally, if $r' \leqslant r$ then

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

Note that the simulation is only in one direction as, in general, if $r' \leqslant r$ then $n[P]^{\mathtt{m}}_{l,r'}$ cannot simulate a broadcast transmission by $n[P]^{\mathtt{m}}_{k,r}$: an observer located at a distance r'', with $r' < r'' < r$, might be able to distinguish the two nodes.

Range repeaters. The next property is about *range repeaters* (or range extenders), and involves stationary nodes, like *access points*. In a wireless network a range repeater 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 that receives messages at channel c and retransmits them on the same channel; the tag $\mathtt{s}$ says that this is a stationary node. Now, suppose we want to extend the range of an access point $n[P]^{\mathtt{s}}_{k,r}$ to cover the cell with center at l and radius r'. In this case, if the distance between k and l is smaller than r and r', respectively, then we could place at l a range repeater with transmission radius r' that simply repeats the signal back and forth. In such a scenario, if node n uses only channel c, then the system composed by the access point at k together with the range repeater at l simulates the presence of the access point at l, with transmission radius r'. More formally,

$$n[P]^{\mathtt{s}}_{k,r} \mid \mathrm{rr}[c \hookrightarrow c]^{\mathtt{s}}_{l,r'} \text{ simulates } n[P]^{\mathtt{s}}_{l,r'}$$

where $\mid$ denotes the parallel composition of nodes.

These examples, together with the others appearing in Section 6, show that our notions of simulation and bisimulation are adequate to prove non-trivial properties of MANETS. However, the experience with other process calculi tells us that there are several different ways to define a bisimilarity. So, the question is: Can we consider our bisimilarity as the natural behavioural equivalence for our calculus? To answer this question we prove that our labelled bisimilarity is a complete characterisation of *reduction barbed congruence*, a standard branching-time and contextually-defined program equality. Reduction barbed congruence is defined as the largest symmetric relation that:

Table 1
The syntax.

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
	$\mid (\nu c)M$	Channel restriction
	$\mid n[P]^{\mu}_{l,r}$	Node (or device)
Processes:		
P,Q,R	$::= \mathbf{0}$	Inactive process
	$\mid c(x).P$	Input
	$\mid \overline{c}\langle w\rangle.P$	Output
	$\mid [w_1 = w_2]P,Q$	Matching
	$\mid A\langle \tilde{w}\rangle$	Recursion
Mobility tags:		
μ	$::= \mathtt{m}$	Mobile
	$\mid \mathtt{s}$	Stationary

- is preserved by all the constructs of the language;
- is preserved (in a sense we will make precise later) by the Reduction Semantics of the language;
- preserves the observables of the language.

Reduction barbed congruence was first studied by Honda and Yoshida [8] under the name of *maximum sound theory*, and it is also known as *open barbed bisimilarity* [24], a slight variant of Milner and Sangiorgi's *barbed congruence* [14].

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*; r for *transmission radii*; x,y,z for *variables*. *Closed values* contain nodes, locations, transmission radii and in general, any basic value (booleans, integers, etc.). *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. 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 is $\mathtt{m}$ 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 6, we also assume some intuitive meta-operators on locations. Network $\mathbf{0}$ denotes the empty network. $M_1 \mid M_2$ represents the parallel composition of two networks. In $(\nu c)M$ the channel c is private to the nodes of M. The restriction operator $(\nu c)M$ models channel restriction but not channel creation.

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. We write $\{^{v}/_{x}\}P$ for the substitution of x with v in P. The output process $\overline{c}\langle v\rangle.P$ can send the (closed) value v via channel c and continue as P. Process $[w_1 = w_2]P,Q$ is the standard "if then else": it behaves as P if $w_1 = w_2$, and as Q otherwise. We write $A\langle \tilde{w}\rangle$ to denote a process defined via a (possibly recursive) definition $A(\tilde{x}) \stackrel{\text{def}}{=} P$, with $\mid \tilde{x} \mid = \mid \tilde{w} \mid$, where $\tilde{x}$ contains all channels and variables that appear free in P. 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 $(\nu c)M$ 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 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. We assume that there are no free variables in a network (while there can be free channels). The absence of free

Table 2
Structural Congruence.

$n[[v = v]P,Q]^{\mu}_{l,r} \equiv n[P]^{\mu}_{l,r}$	(Struct Then)
$n[[v_1 = v_2]P,Q]^{\mu}_{l,r} \equiv n[Q]^{\mu}_{l,r}$ if $v_1 \neq v_2$	(Struct Else)
$n[A\langle\tilde{v}\rangle]^{\mu}_{l,r} \equiv n[\{\tilde{v}/\tilde{x}\}P]^{\mu}_{l,r}$ if $A(\tilde{x}) \stackrel{\text{def}}{=} P \wedge \mid \tilde{x} \mid = \mid \tilde{v} \mid$	(Struct Rec)
$M \mid N \equiv N \mid M$	(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)
$(\nu c)\mathbf{0} \equiv \mathbf{0}$	(Struct Zero Res)
$(\nu c)(\nu d)M \equiv (\nu d)(\nu c)M$	(Struct Res Res)
$c \notin \mathrm{fc}(M)$ implies $(\nu c)(M \mid N) \equiv M \mid (\nu c)N$	(Struct Res Par)
$M \equiv M$	(Struct Refl)
$M \equiv N$ implies $N \equiv M$	(Struct Symm)
$M \equiv M' \wedge M' \equiv M''$ implies $M \equiv M''$	(Struct Trans)
$M \equiv N$ implies $M \mid M' \equiv N \mid M'$, for all M'	(Struct Cxt Par)
$M \equiv N$ implies $(\nu c)M \equiv (\nu c)N$, for all c	(Struct Cxt Res)

Table 3
Reduction Semantics.

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

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

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

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.

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

$$C[\cdot] \ ::= \ [\cdot] \ \mid \ [\cdot] \mid M \ \mid \ M \mid [\cdot] \ \mid \ (\nu c)[\cdot] \ .$$

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 $(\nu \tilde{c})M$ as an abbreviation for $(\nu c_1)\ldots(\nu c_k)M$. 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 $[w_1 = w_2]P,\mathbf{0}$.

2.1. Reduction Semantics

The dynamics of the calculus is specified by the *reduction relation* over networks, $\multimap$, 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 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; δ denotes the maximum distance that a node can cover in a computational step. Notice that stationary nodes cannot move. The remaining rules are standard in process calculi.

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

Table 4
Labelled Transition System—Processes.

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

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

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

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 [12] and in π-calculus [13], 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 receives a particular broadcast 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! As a consequence, 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. Following Milner and Sangiorgi [14] we use the term "barb" as synonymous of observable.

Definition 2.1 (*Barb*)**.** Let K be a set of physical locations. We write $M \downarrow_{c@K}$ if $M \equiv (\nu\tilde{d})(n[\overline{c}\langle v\rangle.P]^{\mu}_{l,r} \mid M')$, with $c \notin \tilde{d}$ and $\mathrm{d}(l,k) \leqslant r$, for all $k \in K$. We write $M \Downarrow_{c@K}$ if $M \multimap^{*} M' \downarrow_{c@K}$.

We also write $M \downarrow_{c@k}$ (respectively, $M \Downarrow_{c@k}$) instead of $M \downarrow_{c@\{k\}}$ (respectively, $M \Downarrow_{c@\{k\}}$).

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 $M \multimap M'$ imply the existence of some N' such that $N \multimap^{*} N'$ 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*)**.** 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:

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

Table 5
Labelled Transition System—Networks.

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

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

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

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

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

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 $\mathrm{d}(l,l') \leqslant r$ guarantees that only nodes within the transmission cell of the transmitter may hear the communication. Rule (Obs) models the fact that every action $c!v[l,r]$ may be detected (and hence *observed*) by any node located in the transmission cell 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 in K. This is an observable action corresponding to the barb $\downarrow_{c@K}$ (see Theorem 3.3(1)): one can imagine a distributed observer seated at each location of K, listening on channel c, and receiving the same value v at each location. 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 process 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; again δ represents the maximum distance that a node can cover in a single computational step. Rule (Par) and (Res) are standard in process calculi. Note that for $\lambda \neq \tau$ rule (Par) can also model the situation where potential receivers do not receive broadcast messages. Note that since we do not transmit channels there is no scope extrusion.

We end this section proving that the LTS-based semantics coincides with the reduction semantics and the notion of observability (barb) given in the previous section. With this objective, we first prove that if $M \xrightarrow{\lambda} N$, then the structure of M and N can be determined up to structural congruence.

Lemma 3.1

(1) *If* $M \xrightarrow{c?v@l} M'$ *then there are* n,P,μ,l,r,M_1, *and* $\tilde{d}$, *with* $c \notin \tilde{d}$, *such that* $M \equiv (\nu\tilde{d})\big(n[c(x).P]^{\mu}_{l,r} \mid M_1\big)$ *and* $M' \equiv (\nu\tilde{d})\big(n[\{^{v}/_{x}\}P]^{\mu}_{l,r} \mid M_1\big)$.

(2) *If* $M \xrightarrow{c!v[l,r]} M'$ *then there are* n,P,μ,l,r,M_1,I (*possibly empty*) *and* $\tilde{d}$, *with* $c \notin \tilde{d}$, *and* n_i,P_i,μ_i,r_i,l_i, *with* $\mathrm{d}(l,l_i) \leqslant r$, *for all* $i \in I$, *such that*

$$M \equiv (\nu\tilde{d})\big(n[\overline{c}\langle v\rangle.P]^{\mu}_{l,r} \mid \prod_{i\in I} n_i[c(x_i).P_i]^{\mu_i}_{l_i,r_i} \mid M_1\big)$$

and

$$M' \equiv (\nu\tilde{d})\big(n[P]^{\mu}_{l,r} \mid \prod_{i\in I} n_i[\{^{v}/_{x_i}\}P_i]^{\mu_i}_{l_i,r_i} \mid M_1\big)\ .$$

Proof. By induction on the transition rules of Table 5. □

We also need to show that structural congruence respects the transitions of Table 5.

Lemma 3.2 ($\equiv$ *respects transitions*). *If* $M \xrightarrow{\lambda} M'$ *and* $M \equiv N$ *then there exists* N' *such that* $N \xrightarrow{\lambda} N'$ *and* $M' \equiv N'$.

Proof. We outline the proof, which proceeds by induction on the depth of the inference $M \xrightarrow{\lambda} M'$. It is enough to prove the result when $M \equiv N$ is due to a single application of a structural rule from Table 2; the general case follows just by iterating the special case. The full proof must treat all possible cases for the final step of the inference $M \xrightarrow{\lambda} M'$. Here we consider just one case; suppose that it is inferred by rule (Par), where M is $M_1 \mid M_2$ and M' is $M_1' \mid M_2$. with $M_1 \xrightarrow{\lambda} M_1'$ inferred by a shorter inference. Now there are many ways in which $M_1 \mid M_2 \equiv Q$ may be due to a single use of a structural congruence rule; we will confine ourselves to considering just two cases.

Case 1. Suppose that the commutativity rule of Table 2 is used, so that N is $M_2 \mid M_1$. In this case we use the rule (Par) to deduce that $N \xrightarrow{\lambda} M_2 \mid M_1'$. Now, take N' to be $M_2 \mid M_1'$; we have $M' \equiv N'$, as required.

Case 2. Suppose that a single rule of structural congruence is used within M_1, so that $M_1 \equiv N_1$ and N is $N_1 \mid M_2$. Then, since $M_1 \xrightarrow{\lambda} M_1'$ is inferred by a shorter inference, by appeal to induction we have $N_1 \xrightarrow{\lambda} N_1'$ and $M_1' \equiv N_1'$. Now take N' to be $N_1' \mid M_2$; by using rule (Par) we deduce that $N \xrightarrow{\lambda} N'$ and $M' \equiv N'$, as required.

So the result follows by a fairly lengthy case analysis, both for the structural congruence rule used and for the last step of the transition inference. □

Theorem 3.3 (*Harmony Theorem*)

(1) $M \downarrow_{c@K}$ *iff* $M \xrightarrow{c!v@K}$ *for some value* v.
(2) *If* $M \xrightarrow{\tau} M'$ *then* $M \multimap\!\triangleright M'$.
(3) *If* $M \multimap\!\triangleright M'$ *then* $M \xrightarrow{\tau} \equiv M'$.

Proof. The first part follows from Definition 2.1 and Lemma 3.1(2).

The second part is by induction on the derivation $M \xrightarrow{\tau} M'$. We recall that the τ-transitions can only be generated by the rules in Table 5.

Suppose that the τ-action has been generated by an application of rule (Lose). In this case, we have $M \xrightarrow{c!v[l,r]} M'$ for some c, v, l, and r. By an application of Lemma 3.1(2) we get:

$$M \equiv (\nu \tilde{d})\big(n[\overline{c}\langle v\rangle.P]^{\mu}_{l,r} \mid \prod_{i\in I} n_i[c(x_i).P_i]^{\mu_i}_{l_i,r_i} \mid M_1\big)$$

and

$$M' \equiv (\nu \tilde{d})\big(n[P]^{\mu}_{l,r} \mid \prod_{i\in I} n_i[\{v/x_i\}P_i]^{\mu_i}_{l_i,r_i} \mid M_1\big)$$

for some n, v, P, μ, l, r, M_1, $\tilde{d}$, with $c \notin \tilde{d}$, and some n_i, P_i, μ_i, r_i, l_i, such that $\mathrm{d}(l,l_i) \leqslant r$, for all $i \in I$. By applying rules (R-Bcast), (R-Par), and (R-Res) we get

$$(\nu \tilde{d})\big(n[\overline{c}\langle v\rangle.P]^{\mu}_{l,r} \mid \textstyle\prod_{i\in I} n_i[c(x_i).P_i]^{\mu_i}_{l_i,r_i} \mid M_1\big) \multimap\!\triangleright (\nu \tilde{d})\big(n[P]^{\mu}_{l,r} \mid \textstyle\prod_{i\in I} n_i[\{v/x_i\}P_i]^{\mu_i}_{l_i,r_i} \mid M_1\big)\ .$$

By applying rule (R-Struct) we obtain $M \multimap\!\triangleright M'$, as required.

Suppose now that that the τ-action $M \xrightarrow{\tau} M'$ has been generated by an application of rule (Move). Then, by an application of rule (R-Move) we derive that $M \multimap\!\triangleright M'$, as required.

The other cases follow from the congruence rules of the reduction relation.

The third part of the theorem is proved by induction of the derivation $M \multimap\!\triangleright M'$.

Suppose that the derivation $M \multimap\!\triangleright M'$ has been generated by an application of rule (R-Bcast), that is,

$$n[\overline{c}\langle v\rangle.P]^{\mu}_{l,r} \mid \prod_{i\in I} n_i[c(x_i).P_i]^{\mu_i}_{l_i,r_i} \ \multimap\!\triangleright\ n[P]^{\mu}_{l,r} \mid \prod_{i\in I} n_i[\{v/x_i\}P_i]^{\mu_i}_{l_i,r_i}$$

such that $\mathrm{d}(l,l_i) \leqslant r$, for all $i \in I$. Then, the derivation below is valid.

$$\dfrac{\dfrac{\overline{c}\langle v\rangle.P \xrightarrow{\overline{c}v} P}{n[\overline{c}\langle v\rangle.P]^{\mu}_{l,r} \xrightarrow{c!v[l,r]} n[P]^{\mu}_{l,r}} \qquad \dfrac{c(x_1).P_1 \xrightarrow{cv} \{v/x_1\}P_1}{n_1[c(x_1).P_1]^{\mu_1}_{l_1,r_1} \xrightarrow{c?v@l_1} n_1[\{v/x_1\}P_1]^{\mu_1}_{l_1,r_1}}}{n[\overline{c}\langle v\rangle.P]^{\mu}_{l,r} \mid n_1[c(x_1).P_1]^{\mu_1}_{l_1,r_1} \xrightarrow{c!v[l,r]} n[P]^{\mu}_{l,r} \mid n_1[\{v/x_1\}P_1]^{\mu_1}_{l_1,r_1}}$$

By applying $|I|-1$ times rule (Bcast) and one time rule (Lose) we get:

$$n[\overline{c}\langle v\rangle.P]^{\mu}_{l,r} \mid \prod_{i\in I} n_i[c(x_i).P_i]^{\mu_i}_{l_i,r_i} \quad \stackrel{\tau}{\longrightarrow} \quad n[P]^{\mu}_{l,r} \mid \prod_{i\in I} n_i[\{v/x_i\}P_i]^{\mu_i}_{l_i,r_i}$$

as required.

Suppose that the derivation $M \multimap M'$ has been generated by an application of rule (R-Move), in this case, by an application of rule (Move) we have $M \stackrel{\tau}{\longrightarrow} M'$.

Suppose that the derivation $M \multimap M'$ has been generated by an application of rule

$$\text{(R-Struct)}\ \frac{M \equiv N \quad N \multimap N' \quad N' \equiv M'}{M \multimap M'}\ .$$

The induction hypothesis tells us that there is N'' such that $N \stackrel{\tau}{\longrightarrow} N'' \equiv N'$. Lemma 3.2 tells us that there is M'' such that $M \stackrel{\tau}{\longrightarrow} M''$ and $M'' \equiv N''$. By transitivity of $\equiv$, it follows that $M \stackrel{\tau}{\longrightarrow} \equiv M'$, as required.

Finally, as both the τ-transitions and the structural congruence are preserved by networks contexts, the cases when the reduction $M \multimap M'$ is derived either by rule (R-Par) or by rule (R-Res) are straightforward. □

4. Bi-simulation proof methods

In this section, we use our LTS to define an appropriate notion of simulation/bisimulation for ad hoc networks. We then prove that our labelled bisimilarity implies reduction barbed congruence, and hence represents a valid method for proving that two networks are reduction barbed congruent.

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

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

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 $\stackrel{\tau}{\longrightarrow}$;
- $\stackrel{c?v@l}{\Longrightarrow}$ denotes $\Rightarrow \stackrel{c?v@l}{\longrightarrow} \Rightarrow$;
- $\stackrel{c!v@K}{\Longrightarrow}$ denotes $\Rightarrow \stackrel{c!v@K_1}{\longrightarrow} \Rightarrow \ldots \Rightarrow \stackrel{c!v@K_n}{\longrightarrow} \Rightarrow$, for $\bigcup_{i=1}^{n} K_i = K$;
- $\stackrel{\hat{\alpha}}{\Longrightarrow}$ denotes $\Rightarrow$ if $\alpha = \tau$ and $\stackrel{\alpha}{\Longrightarrow}$ otherwise.

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

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

- If $M \stackrel{\alpha}{\longrightarrow} M'$, $\alpha \neq c?v@l$, then there is N' such that $N \stackrel{\hat{\alpha}}{\Longrightarrow} N'$ and $M'\ \mathcal{R}\ N'$;
- If $M \stackrel{c?v@l}{\longrightarrow} M'$ then there is N' such that:
  - either $N \stackrel{c?v@l}{\Longrightarrow} N'$ 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.

Remark 4.2. An equivalent way to model the non-observability of message reception is that of adding in the LTS the rule

$$\text{(Shh Rcv)}\ \frac{M \stackrel{c?v@l}{\longrightarrow} M'}{M \stackrel{\tau}{\longrightarrow} M'}$$

to turn message receptions into silent actions. Then, we could completely remove the clause for message reception from Definition 4.1. In the current article, we have preferred to emphasise the non-observable nature of message reception at bisimulation level.

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

(1) $M \mid O \approx N \mid O$, *for all networks O;*
(2) $(\nu c)M \approx (\nu c)N$, *for all channels c.*

Proof. As regards the first item, i.e., that $\approx$ is preserved by parallel composition, we prove that the relation

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

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 $\mathrm{d}(l,k) \leqslant r$, 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 $\mathrm{d}(l,l') \leqslant r$ 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 $N \stackrel{c!v@K'}{\Longrightarrow} N'$ 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 $1 \leqslant j \leqslant n$. 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 $\mathrm{d}(l_j,k) \leqslant r_j$, 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 $\xrightarrow{c!v[l_j,r_j]}$ into $\xrightarrow{c!v@K_j}$. This implies $N \mid O \stackrel{c!v@K}{\Longrightarrow} N' \mid O'$ with $(M' \mid O', N' \mid O') \in \mathcal{S}$, 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 $\mathrm{d}(l,l') \leqslant r$ and $\hat{M} = M' \mid O'$. As $M \approx N$ there is N' such that:
  - either $N \stackrel{c?v@l'}{\Longrightarrow} N'$, 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 $N \mid O \stackrel{c!v@K}{\Longrightarrow} N' \mid O'$, with $(M' \mid O', N' \mid O') \in \mathcal{S}$, 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 $N \mid O \stackrel{c!v@K}{\Longrightarrow} N' \mid O'$, with $(M' \mid O', N' \mid O') \in \mathcal{S}$, 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 order to prove that $\approx$ is preserved by restriction, it suffices to show that the relation

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

is a bisimulation. We do a case analysis on the transition $(\nu c)M \xrightarrow{\alpha} O$. The proof is straightforward as channels cannot be transmitted and hence there is no scope extrusion. □

We can now demonstrate 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 (by Theorems 3.3(2) and 3.3(3)), barb-preserving (by Theorem 3.3(1)), and contextual (by Lemma 4.3). Thus, $\approx \subseteq \cong$. □

5. Characterising reduction barbed congruence

In this section, we prove that our 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 (see for instance [24]).

Proposition 5.1. *If $M \cong N$ then*

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

Lemma 5.2 (*Completeness*)**.** *Reduction barbed congruence is contained in the bisimilarity.*

Proof. We prove that the relation $\mathcal{R} = \{(M,N) \mid M \cong N\}$ is a bisimulation. The result will then follow by co-induction.

- Suppose that $M \mathcal{R} N$ and $M \xrightarrow{\tau} M'$. This case is easy to deal with.
- 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 $\mathrm{d}(l,k) \leqslant r$, 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 $1 \leqslant i \leqslant n$, and channel names f_i and ok_i, for $1 \leqslant i \leqslant n$, 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 $1 \leqslant i \leqslant n$.
  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 $1 \leqslant i \leqslant n$.
  The constraints 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

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

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

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

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

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

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

- Suppose that $M \mathcal{R} N$ and $M \xrightarrow{c?v@l} M'$. We recall that this actions cannot be directly observed, as exemplified by the presence of weaker requirements in the clause for inputs in Definition 4.1. However, a context associated to the action $c?v@l$ could be

$$C[\cdot] \stackrel{\text{def}}{=} [\cdot] \mid n[\overline{c}\langle v\rangle.\overline{\mathsf{f}}\langle v\rangle.\overline{\mathsf{ok}}\langle v\rangle]^{\mathtt{s}}_{k,r}$$

with f and ok fresh channels, and $\mathrm{d}(l,k) \leqslant r$.

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

$$C[M] \;\Rightarrow\; M' \mid n[\overline{\mathsf{ok}}\langle v\rangle]^{\mathtt{s}}_{k,r} = \hat{M}$$

with $\hat{M} \not\downarrow_{\mathsf{f}@k}$ and $\hat{M} \downarrow_{\mathsf{ok}@k}$.

The reduction sequence above must be matched by a corresponding reduction sequence $C[N] \Rightarrow \hat{N}$ with $\hat{M} \cong \hat{N}$, $\hat{N} \not\downarrow_{\mathsf{f}@k}$ and $\hat{N} \downarrow_{\mathsf{ok}@k}$. The constrains on the barbs allow us to deduce the structure of the above reduction sequence. That is:

$$C[N] \Rightarrow N' \mid n[\overline{\mathsf{ok}}\langle v\rangle]^{\mathtt{s}}_{k,r} \cong \hat{N} \ .$$

However, this does not ensure us that N actually performed the $c?v@l$ actions. We can only conclude that there is N' such that either $N \xRightarrow{c?v@l} N'$ or $N \Rightarrow N'$, in case rule (Lose) has been applied to node n.

As $\hat{M} \cong \hat{N}$ and $\cong$ is preserved by restriction it follows that

$$(\nu\mathsf{ok})\hat{M} \cong (\nu\mathsf{ok})\hat{N}$$

from which we can easily derive $M' \cong N'$, as required. □

An easy consequence of Theorem 4.4 and Lemma 5.2 is the following.

Theorem 5.3 (*Characterisation*). *Bisimilarity and reduction barbed congruence coincide.*

6. Properties and examples

In this section, we prove a number of properties using our observational theory. We start proving an interesting property of mobile nodes.

Theorem 6.1 (*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

$$\mathcal{S} \stackrel{\text{def}}{=} \{\, (n[P]^{\mathtt{m}}_{k,r}, n[P]^{\mathtt{m}}_{l,r}) \;:\; \text{for all } P,k,l,r \,\} \cup \mathcal{I}$$

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

Suppose that $n[P]^{\mathtt{m}}_{k,r} \xrightarrow{\alpha} M$, for some α and M, then $n[P]^{\mathtt{m}}_{l,r} \stackrel{\hat{\alpha}}{\Longrightarrow} M$ by applying rule (Move) to migrate to k before performing action α. □

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

Theorem 6.2 (*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 6.3 (*Mixing up infinite output sequences*). *Let* $\mathrm{ALT}(a,b) \stackrel{\text{def}}{=} \overline{c}\langle a\rangle.\overline{c}\langle b\rangle.\mathrm{ALT}\langle a,b\rangle$. *Then, for any l,n,r,u, and v it holds that*:

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

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

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

where $\mathcal{I}$ is the identity relation, is a bisimulation up to $\equiv$. Let us focus on the most significant case. Suppose that

$$n[\,\mathrm{ALT}\langle u,v\rangle]^{\mathrm{m}}_{k,r} \xrightarrow{c!u@K} \equiv n[\,\mathrm{ALT}\langle v,u\rangle]^{\mathrm{m}}_{k,r}$$

for some set of locations K, then

$$n[\,\mathrm{ALT}\langle v,u\rangle]^{\mathrm{m}}_{l,r} \xRightarrow{c!u@K} \equiv n[\,\mathrm{ALT}\langle v,u\rangle]^{\mathrm{m}}_{k,r}$$

by applying rule (Move) to go to location l, rule (Lose) to discard the message v, and rule (Obs) to broadcast value u. □

This result can be generalised by 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 6.4 (*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* $\mathrm{ALT}(a,b) \stackrel{\text{def}}{=} \overline{c}\langle a\rangle.\overline{c}\langle b\rangle.\,\mathrm{ALT}\langle a,b\rangle$. *Then,*

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

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

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

for all l and r, and for all P such that $\mathrm{fc}(P) \subseteq \{c\}$ and $\mathrm{op}(P) \subseteq \{u,v\}$. Let us fix arbitrary u, v, l, and r. Then it suffices to prove that the binary relation

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

is a bisimulation up to $\equiv$. □

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

The next results are about *range repeaters* (or range extenders), and concern 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 network 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 $\mathrm{rr}[c \hookrightarrow c]^{\mathrm{s}}_{l,r}$, where the process $c \hookrightarrow c$ is a forwarder process whose general recursive definition is

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

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 $n[P]^{\mathtt{s}}_{k,r}$. In particular, suppose we want to cover the cell with center at l and radius r'. In this case, if $\mathrm{d}(k,l) \leqslant r$ and $\mathrm{d}(k,l) \leqslant r'$ 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., $n[P]^{\mathtt{s}}_{l,r'}$.

Theorem 6.5 (*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 $\mathrm{d}(k,l) \leqslant r$ and $\mathrm{d}(k,l) \leqslant r'$. Then, the system*

$$n[P]^{\mathtt{s}}_{k,r} \mid \mathrm{rr}[c \hookrightarrow c]^{\mathtt{s}}_{l,r'}$$

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

Proof. By proving that the relation

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

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 channel, which effectively doubles the number of frames that are sent. In particular, whenever the range repeater transmits on channel c the node n must remain silent to avoid collisions. A way to avoid this inconvenience 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 6.6 (*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,r' be transmission radii, such that $\mathrm{d}(k,l) \leqslant r$ and $\mathrm{d}(k,l) \leqslant r'$. Then, for any channel d, the system*

$$n[P]^{\mathtt{s}}_{k,r} \mid \mathrm{out}[c \hookrightarrow d]^{\mathtt{s}}_{l,r'} \mid \mathrm{in}[d \hookrightarrow c]^{\mathtt{s}}_{l,r'}$$

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

Proof. We prove that the relation

$$\begin{array}{rcl}\mathcal{S} & \stackrel{\mathrm{def}}{=} & \{\Big(n[\{^{d}/_{c}\}P]^{\mathtt{s}}_{l,r'}\,,\, (n[P]^{\mathtt{s}}_{k,r} \mid \mathrm{out}[c \hookrightarrow d]^{\mathtt{s}}_{l,r'} \mid \mathrm{in}[d \hookrightarrow c]^{\mathtt{s}}_{l,r'})\Big) : \\ & & \quad \forall\, k,l,r,r'.\ \mathrm{d}(k,l)\leqslant r \,\wedge\, \mathrm{d}(k,l)\leqslant r' \\ & & \quad \forall\, P.\ \mathrm{fc}(P) \subseteq \{c\} \\ & & \} \end{array}$$

is a simulation. □

As already pointed out, the previous results on range repeaters only regards stationary nodes. In fact, range repeaters are superfluous when dealing with mobile nodes, as exemplified below.

Theorem 6.7. *Let k,l be physical locations and r,r' be transmission radii such that $r \geqslant r'$. Then,*

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

Proof. We show that the relation

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

is a simulation. □

Finally, we provide a result concerning 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 $\frac{p_k}{\mathrm{d}(k,l)^{\alpha}} \geqslant \beta$, where $\alpha \geqslant 2$ is the *distance-power gradient* and $\beta \geqslant 1$ is the *transmission quality* parameter.[1] 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.

[1] 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.

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 6.8 (*Saving antenna power*). *Let P 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 $\mathrm{d}(l_1,l_2) = r$, with $r \leqslant r_1$ and $r \leqslant r_2$. Then, the system*

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

simulates the system

$$(\nu d)\big(m[P]^{\mathrm{s}}_{l_1,r_1} \mid n[Q]^{\mathrm{s}}_{l_2,r_2}\big)\ .$$

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

$$\begin{array}{lll}\mathcal{S} & \stackrel{\mathrm{def}}{=} \{ & \Big((\nu d)(m[P]^{\mathrm{s}}_{l_1,r_1} \mid n[Q]^{\mathrm{s}}_{l_2,r_2}), (\nu d)(m[P]^{\mathrm{s}}_{l_1,r/2} \mid \mathrm{rr}\,[d \hookrightarrow d]^{\mathrm{s}}_{l_1+r/2,r/2} \mid n[Q]^{\mathrm{s}}_{l_2,r_2})\Big) : \\ & & \forall\, l_1,l_2,r_1,r_2.\ \ \mathrm{d}(l_1,l_2) \leqslant r_1 \ \wedge\ \mathrm{d}(l_1,l_2) \leqslant r_2 \\ & & \forall\, Q\ \forall P.\ \ \mathrm{fc}(P){=}\{d\} \\ & \} & \end{array}$$

is a simulation. The most significant case is when the nodes n and m of the system

$$(\nu d)\big(m[P]^{\mathrm{s}}_{l_1,r_1} \mid n[Q]^{\mathrm{s}}_{l_2,r_2}\big)$$

communicate via channel d. Then, the presence of the range repeater in the system

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

allows to simulate the communication. □

Notice that the result does not hold if we remove the restriction on channel d. This is because our transmission cells are meant to have a circular shape. Had the signal propagation be directional then the result would hold without the restriction on channel d.

7. Related and future work

Broadcast for Ethernet-like communications has been first analysed by Prasad [20,21,16] in his *Calculus of Broadcasting Systems* (CBS), in which all processes receive a broadcast message at once. In [19] 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 [7] 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 [15] 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 similar to that of [19,7] 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 et al. [26] have designed 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.

More recently, Godskesen [5] has proposed CMAN, a name-passing calculus for ad hoc networks without channel restriction, and where nodes can be hidden to the environment. In CMAN the neighbourhood's relation is given in terms of logical locations letting the topology be explicit part of the network syntax. The paper provides a labelled bisimilarity that characterises reduction barbed congruence. The labelled bisimilarity is then used to formalise an attack on the cryptographic routing protocol ARAN [25].

Finally, notice that all the previous calculi abstract from interferences. Mezzetti and Sangiorgi [10] 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 [10], the reduction semantics and the corresponding LTS is quite different; this is because in our model we assume the absence of interferences.

A number of developments are possible. For instance, we could enrich the calculus with operators to model the concept of store as in [15]. 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 [6], SCCS [11]). 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 [15], security is, of course, another important issue in MANETs that we would like to investigate.

8. Acknowledgments

We thank the anonymous reviewers for valuable comments. We thank Davide Sangiorgi for insightful remarks on a early draft. Thanks to Davide Quaglia for interesting discussions on MANETs.

References

[1] G. Berry, G. Gonthier, The esterel synchronous programming language: design, semantics, implementation, Science of Computer Programming, 19 (2) (1992) 87–152.
[2] C. Ene, T. Muntean, A broadcast based calculus for communicating systems, in: IPDPS, IEEE Computer Society, 2001, pp. 149–159.
[3] A. Francalanza, 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, pp. 368–382.
[4] A. Francalanza, M. Hennessy, A theory for observational fault tolerance, in: FoSSaCS, volume 3921 of Lecture Notes in Computer Science, Springer, 2006, pp. 16–31.
[5] J.C. Godskesen, A calculus for mobile ad hoc networks, in: COORDINATION, volume 4467 of Lecture Notes in Computer Science, Springer Verlag, 2007, pp. 132–150.
[6] D. Harel, Statecharts: a visual formulation for complex systems, Science of Computer Programming 8 (3) (1987) 231–274.
[7] M. Hennessy, J. Rathke, Bisimulations for a calculus of broadcasting systems, Theoretical Computer Science 200 (1998) 225–260.
[8] K. Honda, N. Yoshida, On reduction-based process semantics, Theoretical Computer Science 152 (2) (1995) 437–486.
[9] M. Merro, An observational theory for mobile ad hoc networks, Electronic Notes in Theoretical Computer Science 173 (2007) 275–293.
[10] N. Mezzetti, D. Sangiorgi, Towards a calculus for wireless systems, Electronic Notes in Theoretical Computer Science 158 (2006) 331–353.
[11] R. Milner, Calculi for synchrony and asynchrony, Theoretical Computer Science 25 (1983) 267–310.
[12] R. Milner, Communication and Concurrency, Prentice Hall, 1989.
[13] R. Milner, J. Parrow, D. Walker, A calculus of mobile processes (parts I and II), Information and Computation 100 (1992) 1–77.
[14] R. Milner, D. Sangiorgi, Barbed bisimulation, in: ICALP, volume 623 of Lecture Notes in Computer Science, Springer Verlag, 1992, pp. 685–695.
[15] S. Nanz, C. Hankin, A framework for security analysis of mobile wireless networks, Theoretical Computer Science 367 (1-2) (2006) 203–227.
[16] K. Ostrovsky, K.V.S. Prasad, W. Taha, Towards a primitive higher order calculus of broadcasting systems, in: PPDP, ACM, 2002, pp. 2–13.
[17] C.E. Perkins, E.M. Belding-Royer, Ad-hoc on-demand distance vector routing, in: WMCSA, IEEE Computer Society, 1999, pp. 90–100.
[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 value broadcasts, in: PARLE, volume 694 of Lecture Notes in Computer Science, Springer Verlag, 1993, pp. 391–402.
[20] K.V.S. Prasad, A calculus of broadcasting systems, Science of Computer Programming 25 (2–3) (1995).
[21] K.V.S. Prasad, Broadcasting in time, in: COORDINATION, volume 1061 of Lecture Notes in Computer Science, Springer Verlag, 1996, pp. 321–338.
[22] K.V.S. Prasad, A prospectus for mobile broadcasting systems, in: Workshop on Algebraic Process Calculi: The First Twenty-Five Years and Beyond (PA'05). BRICS Press, 2005.
[23] T. Rappaport, Monographs in Computer Science, second ed., Prentice Hall, 2002.
[24] D. Sangiorgi, D. Walker, The π-Calculus: A Theory of Mobile Processes, Cambridge University Press, 2001.
[25] K. Sanzgir, D. LaFlamme, B. Dahil, B. Neil Levine, C. Shields, E.M. Belding-Royer, Authenticated routing for ad hoc networks, IEEE Journal on Selected Areas in Communication, special issue on Wireless Ad Hoc Networks 23 (3) (2005) 598–610.
[26] A. Singh, C.R. Ramakrishnan, S.A. Smolka, A Process Calculus for Mobile Ad Hoc Networks, 2006. Available from: <http://www.lmc.cs.sunysb.edu/~cram/Papers/SRSOmegaCalc2006/urlhttp://www.lmc.cs.sunysb.edu/~cram/Papers/SRSOmegaCalc2006/>.