A Process Calculus for Energy- Aware Multicast Communications of Mobile Ad-Hoc Networks

Lucia Gallina and Sabina Rossi

Dipartimento di Informatica, Università Ca' Foscari, Venice
{lgallina,srossi}@dsi.unive.it

Abstract. We present E-BUM, a process calculus for formally modelling and reasoning about Mobile Ad Hoc Networks (MANETs) and their protocols. Our calculus naturally captures essential characteristics of MANETs, including the ability of a MANET node to broadcast a message to any other node within its physical transmission range, and to move in and out of the transmission range of other nodes in the network. In order to reason about cost-effective ad hoc routing protocols, we also allow unicast and multicast communications as well as the possibility for a node to control the transmission radius of its communications. We show how to use our calculus in order to prove some useful connectivity properties of MANETS, to manage the problem of reducing interference and to analyse strategies for power administration.

1 Introduction

1.1 Mobile Ad-Hoc Networks

A mobile ad-hoc network (MANET) is a self-configuring network composed of devices connected by wireless links. The network is composed of both mobile and stationary nodes, then its topology may change rapidly and unpredictably, Mobile devices are free to move randomly and organise themselves arbitrarily. Mobile Ad-Hoc Networks are built using wireless technology, the devices communicate with each other via radio transceivers, using the protocol IEEE 802.11 (WiFi) [29]. This type of communication has a physical scope, because a radio transmission spans over a limited area. Therefore it necessarily must be applied a routing protocol, proper to wireless dynamic systems.

As mobile ad hoc networks communicate in a self organized way without depending on any fixed infrastructure, they are the best solution for various applications, ranging from the monitoring of herds of animals to supporting communications in military battlefields and civilian disaster recovery scenarios. Many of these applications require that nodes be mobile and be deployed with little network planning. The mobility of nodes limits their size, which in turn limits the energy reserves available to them. Moreover, in wireless networks, bandwidth is precious and scarce. Thus energy and bandwidth conservation is a key requirement in the design of MANETs.

As MANETs are usually implemented in precarious environments, they are vulnerable to many attacks, because the nodes only communicate using radio-frequency channels, which cannot be private. They are also power limited, because constituted of various devices as mobile phones and notebooks. The dynamic nature of this kind of networks makes the management of the transmissions and of the routing protocol much more complicated. The ad hoc networks are self organized, so the good behavior of the system depends on the cooperation among the connected nodes: this characteristic can make the network more vulnerable to damages caused, not only by malicious nodes, but also by "lazy" nodes, that are devices which, for power saving, do not cooperate with the other nodes; this bad behavior can originate problems especially in the management of the packets routing. Since the Mobile Ad-Hoc networks are used for the management of critical situations, where the transmitted data are often important and confidential, we are now going to enumerate the main properties to be preserved in planning an ad hoc network [30], [3], [21].

Security issues in mobile Ad-Hoc Networks

Authentication
Enables nodes to ensure the identification of the nodes they are communicating with.

Integrity
Guarantees that a message has not be modified or corrupted during its transmission

Confidentiality
Ensures that confidential data are never disclosed to unauthorised entities. In some environments also the information about the physical locations of the nodes must be protected (*Location Confidentiality*).

Availability
Ensures the survivability of network services despite denial of service attacks. On the network layer, an adversary could disrupt the routing protocol to disconnect the network. On the higher layers an adversary could bring down high-level services.

Access control
Guarantees the control of network's data flow.

Non-repudiation
Ensures that a device transmitting a message cannot deny having sent it. This future is useful for the detection of compromised nodes.

No traffic diversion
Ensures a control of the information traffic, protecting the network from malicious nodes and from non-cooperative nodes, that do not forward the messages in order to save power.

Cooperation and fairness
Ensures the cooperations of all the nodes of the network.

Power control
Ensures that any action of a node respects the power capacity of the devices

(the mobile Ad-hoc networks are constituted of many kinds of devices, as mobile phones and notebooks).

Since the Ad-Hoc Networks are often used in critical situations (especially in case of war), it is not important only to preserve the properties we have just enumerated, but it is also necessary to preserve the network from security problems [30], [3], [21]. We are going now to list the possible attacks to a MANET. Any attack on ad hoc networks can be categorized as passive or active attack. In a passive attack the malicious node only listens to the traffic, without disturbing the network, while in an active attack the malicious node disturbs the normal operation of the network.

Attacks to mobile Ad-Hoc Networks

Message tampering attack
A node could intercept and alter the content of a packet, compromising data integrity

Message dropping attack
A malicious node could intercept packets and drop them, hampering the correct communication of the nodes in the network.

Message reply attack
Malicious nodes could eavesdrop on the packets transmitted, and reply those packets again later.

Identity falsification
A node could alterate the information about its identity.

Impersonation
A node could communicate with the network, using the identity of an other device.

Network obstructing attack
A malicious node could generate packets only to overload the network, obstructing the correct communications of the nodes.

Non-cooperation attack
A selfish node, that wants to save power, could refuse to cooperate to the correct packet routing within the network.

Not only malicious or selfish nodes can obstruct the correct behavior of a network, but also nodes that have been compromised by physical damages, which can cause non-cooperations, or the transmission of corrupted data within the network (Consider for example the case of a node whose route table has been compromised: this can produce a series of transmission failures).

1.2 The problem of Power Consumption in Mobile Ad Hoc Networks

In managing power consumption in the ad hoc networks there are several issues to consider:

Network connectivity maintenance if we consider the necessity of reducing power consumption in managing networks transmissions, we have always to consider also the connectivity of nodes: a device cannot use a transmission power that is too small to reach the receivers of its messages

Reduction of Interference Ad hoc networks use radiofrequences to communicate. In particular, when using these technologies, channels are *half-duplex*: a node cannot transmit and receive at the same time. Using too large transmission powers will therefore increase the interference level.

Battery Waste avoidance Ad hoc networks are constituted of different kinds of devices (notebook, mobile phones...) which may have scarce energy capacities, and battery with an autonomy of few hours. When dealing with transmission power we have always to consider also these problems affecting various devices which are party to the communications.

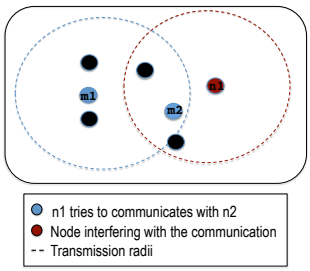
Network capacity Optimisation When dealing with power consumption of ad hoc networks we have to consider, not only the problems and characteristics of the single devices, but also the general characteristics of the whole network, considering the critical environments in which they are often installed, and their employment (often they are installed in order to face emergency situations, as natural disasters or wars).

The concept of *topology control* is the technique used in order to reduce the initial topology of the network to save energy, and to extend the lifetime of the network. This can be then considered as a trade-off between power saving and network connectivity: in other words when we have to choose the transmission power of each node, we know that choosing a low transmission power for a node we will reduce its connectivity within the network, but we also reduce its power consumption. The main goal of topology control is therefore the choice, for each node, of a minimum transmission power which guarantees network connectivity. There is an other problem depending on the transmission power we choose for a node sending data within the network: a too large transmission radius will reach a large number of nodes, and this may increment probability of disturbing devices not interested in receiving the data transmitted, and to congest the network. Moreover in a Wireless Network links may be not bidirectional (devices have not always the same transmission range), and each node is directly connected only with the devices lying within its transmission cell. Following we will illustrate some common critical scenarios arising during a wireless node's transmission, which interferes with its neighbours, possibly blocking their transmissions or receptions.

The problem of the Hidden Station

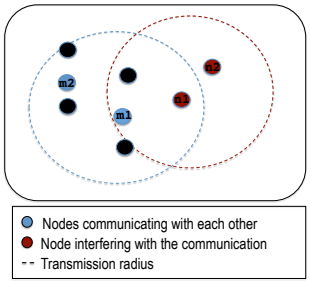
The problem of the Hidden Station arises during a communication: the sender is not able to detect potential nodes competing in transmitting to the same receiver. An example of this kind of problem is shown in Figure 1: n1 tries to transmit to n2; it can only be sure that the channel is free within its transmission area, but it cannot see if n2 is reachable by some other node transmitting at the same time.

Fig. 1: The problem of the Hidden Station



The problem of the Exposed Station

Fig. 2: The problem of the Exposed Station



Another situation which can be generated in networks where channels are half-duplex is when a node is prevented from sending packets to other nodes due to a neighbouring transmitter. Figure 2 shows an example of this kind of situations, which is essentially the opposite one with respect to the Hidden Station problem. The node disturbed is the sender, then it will not transmit (or it will interrupt it soon) and wait, causing a delay on its transmission.

The CSMA protocol

The MAC (Media Access Control) is a sub-layer of Data Link Layer (the second in the ISO/OSI model). It provides Multiple Access protocols, allowing several devices connected to the same physical medium to share it. The behaviour of this layer is interesting especially in dealing with *half-duplex* channels, which do not allow sending and receiving at the same time.

CSMA (Carrier Sense Multiple Access) [26] is the standard protocol used by the MAC layer to manage multiple access channels. "Carrier Sense" describes the fact that a transmitter uses feedback from a receiver that detects a carrier wave before trying to send. That is, it tries to detect the presence of an encoded signal from another station before attempting to transmit. If a carrier is sensed, the station waits for the transmission in progress to finish before initiating its own transmission. "Multiple Access" describes the fact that multiple stations send and receive on the medium. Transmissions by one node are generally received by all other stations using the medium.

CSMA is a probabilistic protocol: a node verifies the absence of traffic in the channel, then it will transmit with a certain probability p. There are two different versions of CSMA:

- **CSMA/CA (CSMA with Collision Avoidance)**
  CSMA with Collision Avoidance is a version of CSMA which tries to completely remove collisions in transmissions. This protocol is especially used when managing wireless networks, and it is enforced by using RTS/CTS (Request To Send and Clear To Send respectively) message exchange.
- **CSMA/CD (CSMA with Collision Detection)**
  CSMA with Collision Detection is a modification of pure Carrier sense multiple access (CSMA) and it is used to improve CSMA performance by terminating a transmission as soon as a collision is detected, and reducing the probability of a second collision on retry. This kind of protocol is used especially for Ethernet. The idea this protocol is based on, is to provide a way of detect and interrupt the "bad transmissions" in a reasonable time interval will lead to power saving (only good transmissions are completely performed).

When dealing with wireless networks the problem of collisions is solved at data link layer by using the CSMA with collision avoidance. Even if collisions are completely removed, there are other problems arising when a node decides to begin a transmission.

The problem of interference is strictly connected with the power consumption: by reducing the power of transmission in a network, we save energy and reduce the transmission area of a node, consequently reducing also the noise provoked by that transmission to the other devices communicating within that network.

1.3 Process calculi studying the behavioural theory of MANETS

Ad hoc networks are still a new branch of wireless communication; many researchers have yet tried to create a process calculus in order to model them correctly, for the analysis of their properties and problems. The first step of this work has been then a bibliographic research choosing one of the process calculi already created for modelling MANETS in order to study it and eventually optimise it with some modifications. We paid particular attention to different

calculi, which we have analysed in parallel evaluating their qualities and defects. All the models we analysed use the *process algebra*, in particular there have been created extensions of calculi as CCS [16] and π-calculus [17], described using LTS semantics (Labelled Transition System). The notions of simulation and bisimulation are always introduced [22], [8], [2]. Properties to be preserved in the realisation of a mobile ad hoc network are various and sometimes contradictory (for example if we need to preserve data integrity we have to ignore the necessity of power saving, while an excessive power saving could compromise network availability and data integrity), so each model has paid attention to a different characteristic of MANET, then the calculi that have been analysed result to be really different from each other.

Jens Chr. Godskesen has proposed CMAN (Calculus for Mobile Ad Hoc Networks) [10], where connections between the nodes of the network is expressed using bidirectional links. A tag is associated to each node, containing the logical locations of the nodes it is connected with. Rules of CMAN allow scope extrusion. Contrarily to the other calculi we found in literature, here the network topology has been represented with bidirectional links between the logical locations of the devices (nodes are not associated to a transmission radius nor a physical location). The author had chosen this solution believing that, dealing with the node's behaviour in its intentions with the network and its neighbours, separately from its physical position, could simplify the model.

Nanz and Hankin have introduced the CBS$^{\#}$ [18], an extension of CBS (Calculus of Broadcasting Systems) [20]; the peculiarity of this calculus is the choice of representing a node as a couple composed of a process and a store associated to a location. This solution allows the representation in detail of the network, that is constituted of devices which have an own store. Nevertheless the actions executed on the store are internal to the node, so they are not observable actions: their representation make the calculus heavy without a real optimisation. The other important peculiarity characterising the CBS$^{\#}$ is that the transmission is not considered an atomic action, but, when a node executes an output action, the topology of the network may change arbitrarily before the reception of the message by the neighbours of the sender. On contrary in the other calculi (as CMN or CMAN) transmissions are considered atomic actions: topology of the network cannot change during a transmission. Notice that, even though the transmission is an atomic action, the input action is not deemed a direct consequence of an output, but information broadcasted to the network can be lost, meaning that no nodes of the network received it.

Merro has introduced CMN [14] (Calculus of Mobile Ad-Hoc Networks), an extension of CCS [16], where the topology of the network is represented by a set of nodes associated with a location and a transmission radius. Contrarily to the other calculi we paid attention to, the connectivity of a node is defined by a physical transmission area, rather than by a group of nodes. This characteristic allows one to describe more in detail the observability of the network, and this is the main reason why we have chosen this calculus as the first step of our work. By a deep analysis of CMN, we found some limitations of this calculus, as the ab-

sence of a rule for arbitrary disconnections and connections of stationary nodes, or the impossibility of representing multicast and unicast communication; even though mobile ad hoc networks use only radio frequencies for communications, which do not allow one to make a channel private, in some cases it is necessary specifying the particular receivers of a message.

We think that Merro gives the best way of representing a node for ad hoc networks, but in our work we have decided to extend that calculus with some modifications in order to make it more expressive, and to be able of study a larger number of properties of mobile ad hoc networks.

Singh, Ramakrishnan e Smolka have designed the ω-calculus [25], a conservative extension of the π-calculus [17]. The key future of this calculus is the separation of a node's communication and computational behavior from the description of its physical transmission range. The latter is modelled annotating a process with the set of group names to which it belongs. Since the ω-calculus is a conservative extension of the π-calculus, *scope extrusion* is defined (nodes can create new names and privately share them with other devices). The peculiarity of this calculus is that not only broadcast transmissions are permitted, but also multicast and unicast communications. The communications in the ad hoc networks are realised using WiFi, so only broadcast transmissions are permitted; however it can result useful a representation of multicast and unicast communication, because some routing protocols use them (as the AODV [6] [23], which is one of the best routing protocol for MANETS) and their realisation is anyway possible using the standard IEEE 802.11. The calculus we propose enables us to represent broadcast, unicast and multicast communications, as well as ω-calculus; however we think that our model better represents the real nature of ad hoc networks: a message sent to a specific group of receivers is not hidden to the rest of the network: in the ω-calculus a multicast communication is represented as private, while we only specify the intended recipients of a transmission, without forgetting that all the network will be able to receive the message anyway.

As the main goal of our work is the power saving in ad hoc network management, we had a look to the stochastic process calculi present in literature, looking for the best way of analysing and evaluating MANETs' protocols performances (in terms of power saving). Literature is rich of stochastic and probabilistic process calculi, as PEPA (Performance Evaluation Process Algebra) [13], introduced by Jane Hilston, which is a timed and stochastic extension of classical process algebras such as CCS [16] that associates a random variable, representing duration, with every action. Goubault-Larrecq, Palamidessi and Troina proposed a probabilistic π-calculus [12], which is an extension of the applied Pi-calculus with the introduction of nondeterministic and probabilistic operators. Although these kinds of calculus have been used for the performance evaluation of many protocols and applications concerning various kinds of networks (including mobile nodes and broadcast, unicast and multicast communications), we have found nothing analysing the specific case of Power saving in Mobile Ad Hoc Networks, while our work, even if it is not a stochastic nor a probabilistic model, gives a good instrument for a performance evaluation of MANETs.

1.4 Contribution

We propose E-BUM (A calculus for Energy-aware Broadcast, Unicast, Multicast communications in Ad Hoc Networks), an extension of CMN [14], defining a new sintax and semantics. Following we enumerate the main contributions of our work.

- The first novelty we introduced is about the output actions, in particular we added a tag constituted of a set of locations. This tag is associated to the channel of the transmission, and it indicates the intended recipients of a packet transmitted. Ad hoc networks use radio-frequencies for the communications, so each packet transmitted will be always receivable by the whole network, because no channels can be private. Nevertheless the specification of the recipients of the messages transmitted allows us to a better analysis of the behaviour of the networks consequently to each transmission; for example we can decide if the transmission radius of the node sending the message is sufficient to reach all the nodes it is addressed to. Using this new tag we can moreover represent unicast and multicast communications; even if channels are not private in mobile ad hoc networks, it is anyway useful a tag specifying which are the nodes that are really interested in receiving a message.
- The second novelty we introduced is the possibility of a node to connect and disconnect arbitrarily. This has be made by enabling nodes to set their transmission radius to the value 0. We think that, by giving a way to arbitrarily connect and disconnect any node of the network is useful because we can represent many kinds of situations, as physical damages to the devices, or the battery wear out.
- The third important novelty we introduced is the possibility for a node to adjust its transmission radius. In particular we use the radius of the nodes as a parameter in order to analyse the power consumption of a transmission, and then study the problem of energy management in ad hoc networks.

In order to prove the usefulness of our model, and the importance of the new characteristics we introduced with respect to the other calculi present in literature, we demonstrate a series of properties concerning connectivity and communications problems in MANETS. We also deal with the problem of interference in Mobile Ad Hoc networks, by giving two different definitions: the former focuses our attention to the noise provoked by a sender during a transmission, while the latter defines the interference as the noise arising at a receiver.

2 E-BUM

In Table 1 we define the sintax of E-BUM. This is defined in a two-level structure: the lower one for processes, the upper one for networks. the channel names set is separated from the names set.

$\mathbf{C}$ = channels set, $d, c \in \mathbf{C}$;

Table 1: **Sintax**

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
	$\mid c(\tilde{x}).P$	Input
	$\mid \bar{c}_{L,r}\langle\tilde{w}\rangle.P$	Output
	$\mid [w_1 = w_2]P, Q$	Matching
	$\mid A\langle\tilde{w}\rangle$	Recursion
Mobility tags		
μ	$::= \mathtt{m}$	Mobile node
	$\mid \mathtt{s}$	Stationary node
Channels' description tags		
L	$::= \{l_1, l_2, l_3, ...\}$	Multicast/unicast channel
	$\mid \infty$	Broadcast channel
	$\mid \epsilon$	Empty channel

$\mathbf{N}$ = names set. In particular letters m, n are used for nodes, l, k, h for locations and r for transmission radii;
$\mathbf{X}$ = variables set (x, y, z);
$\mathbf{V}$ = values set $(\mathbf{X} \cup \mathbf{N} \in \mathbf{V})$;

Values set includes names, variables and in general, any basic value (integers, booleans, etc.). Letters u, v are used for closed values, and w for open values. A tuple $a_1, ..., a_k$ of names is represented by $\tilde{a}$. Networks are collections of nodes (which represent devices), running in parallel, using channels to communicate messages. Network $\mathbf{0}$ denotes empty network. $M_1|M_2$ represents the parallel composition of two networks. In $(\nu c)M$ channel c is private to the nodes of M. The restriction operator models channel restriction but not channel creation.

Processes are sequential and live within the nodes. Process $\mathbf{0}$ denotes inactive processes. The input process $c(\tilde{x}).P$ can receive a tuple of values via channel c and continues as P, with $\tilde{w}$ substituted for $\tilde{x}$. We write $\{\tilde{w}/\tilde{x}\}P$ for the substitution of $\tilde{x}$ with $\tilde{w}$ in P (where $|\tilde{x}| = |\tilde{w}|$). The output process $\bar{c}_{L,r}\langle\tilde{w}\rangle.P$ can send a term $\tilde{w}$ via channel c and continue as P. The tag L is used to list the locations of the recipients of the message transmitted; in particular $L = \infty$ means a broadcast transmission, otherwise the message is transmitted with multicast communication (unicast if the set L has only one member). The tag r associated to an output action represents the radius (and then the power) used to transmit: we consider that in managing ad hoc networks the choice of the transmission power of each device may depend on precise strategies which are implemented in the communication protocols; then it is reasonable considering transmission range as an information given by the process running in the sender node. Syntactically, the tags L and r associated to the channel c in an output action may be variables, but they must be instantiated when the output prefix is ready to fire. Note that a node n will never execute any process P requiring transmission radius $r > r_n$.

Process $[w_1 = w_2]P, Q$ is the standard if-then-else: it behaves as P if $w_1 = w_2$, 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 $|\tilde{x}| = |\tilde{w}|$.

Each node, if connected, 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 (that is the logic location of the device in the network), located at l, with r transmission radius, μ mobility tag, and executing a process P. μ is $\mathtt{m}$ for mobile nodes, and $\mathtt{s}$ for stationary nodes; l denotes the physical location of the node.

The possibility of the nodes to communicate with each other is verified looking at the physical locations and the transmission radii, in other words if a node broadcasts a message, this information will be received only by nodes that lie in the area delimited by the transmission radius of the sender. In the definition of the operational semantics we then assume the possibility of comparing locations so to determine wether a node lies or not within the transmission cell of another node. We do so by means of a function $d(\cdot, \cdot)$ which takes two locations and returns their distance. .

In the process $c(\tilde{x}).P$ variable x is bound in P, giving rise to the standard notions of α-conversion and free and bound variables, denoted by $fv(\cdot)$ and $fb(\cdot)$ 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, $fc(\cdot)$ and $bc(\cdot)$, are defined accordingly.

Processes and networks are then identified up to α-conversion. More formally terms are considered 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 context $\mathcal{C}[\cdot]$ is defined as a network term with a hole, denoted by $[\cdot]$. Contexts are generated by the following grammar:

$$\mathcal{C}[\cdot] ::= [\cdot] \mid [\cdot]|M \mid M|[\cdot] \mid (\nu c)[\cdot] \tag{1}$$

A number of conventions are used to simplify the notation. Parallel composition of networks has lower precedence with respect to restriction. $\prod_{i\in I} M_i$ means the parallel composition of all the networks $M_i, \forall i \in I$. We write $(\nu\tilde{c})M$ as an abbreviation for $(\nu c_1)...(\nu c_k)M$. To denote unicast communication we write c_l for $c_{\{l\}}$. We write $\bar{c}_{L,r}\langle w\rangle$ for $\bar{c}_{L,r}\langle w\rangle.\mathbf{0}$, $\mathbf{0}$ for $n[\mathbf{0}]^\mu_r$ and $[w_1 = w_2]P$ as an abbreviation of $[w_1 = w_2]P, \mathbf{0}$. We assume that there are no free variables in a network (while 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.

Table 2: **Structural Congruence**

$n[[v = v]P, Q]^\mu_{\lambda,r} \equiv n[P]^\mu_{\lambda,r}$	(Struct Then)
$n[[v_1 = v_2]P, Q]^\mu_{\lambda,r} \equiv n[Q]^\mu_{\lambda,r} \quad v_1 \neq v_2$	(Struct Else)
$n[A\langle\tilde{v}\rangle]^\mu_r \equiv n[\{\tilde{v}/\tilde{x}\}P]^\mu_{\lambda,r}$ if $A(\tilde{x}) \stackrel{\text{def}}{=} P \wedge |\tilde{x}| = |\tilde{v}|$	(Struct Rec)
$M\|N \equiv N\|M$	(Struct Par Comm)
$(M\|N)\|M' \equiv M\|(N\|M')$	(Struct Par Assoc)
$M\|\mathbf{0} \equiv M$	(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)
$(\nu c)(M\|N) \equiv M\|(\nu c)N$ If $c \notin fc(M)$	(Struct Res Par)
$M \equiv M$	(Struct Refl)
$N \equiv M$ if $M \equiv N$	(Struct Symm)
$M \equiv M''$ if $M \equiv M' \wedge M' \equiv M''$	(Struct Trans)
$M\|M' \equiv N\|M' \quad \forall M'$ if $M \equiv N$	(Struct Cxt Par)
$(\nu c)M \equiv (\nu c)N \quad \forall c$ if $M \equiv N$	(Struct Cxt Res)

2.1 Reduction Semantics

The dynamics of the calculus are specified by the *Reduction Relation* over networks ($\rightarrow$), 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. Structural congruence brings the participants of a potential interaction into contiguous positions.

Rule (R-Bcast) models the transmission of a tuple of messages $\tilde{v}$ using channel c_L and transmission radius r. Mobile ad hoc networks are always implemented with different kinds of devices, and nodes communicate using radio frequencies, which enable only broadcast of message (monopolising channels is not permitted). Otherwise a node may decide to communicate with a specific node (or group of nodes), this is the reason why we decided to associate each output action with the set of transmission recipients. The cardinality of this set indicates the kind of communication that has been used: if a node broadcasts a message (the recipient is the whole network), it will use a channel tagged with the infinite set (for example c_∞); if the message has only a recipient (unicast transmission), the sender will use a channel as c_l; finally, if the cardinality of L is a finite number more than one there will be a multicast transmission. The recipients set indicates which are the nodes really interested in receiving that particular information, but we know that every message sent from a node will be potentially received by all the devices lying within the transmission cell of the sender, because radio frequencies do not allow one to make a channel private. We have decided to specify anyway the recipients set, to better describe the behaviour of the network during the transmissions. If two nodes want to share a secret, they must use cryptography to hide the message.

In our calculus transmission is a *non-blocking action*: transmission proceeds even if there is no other process listening for messages. This is an instantaneous action and the message transmitted will be received only by those nodes which lie in that instant in the transmission area of the sender. Notice 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 that concern the instability and dynamism of the environments where ad hoc networks are usually installed. In terms of observation this corresponds to a local activity of the network which an external observer is not party to. In this calculus movement is considered an atomic action: while moving, a node cannot do anything else.

Rule (R-Rad) models the possibility for a node n to control power consumption by changing its transmission radius r into r' provided that $r' \in [0, r_n]$.

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. Moreover there are specific rules modelling arbitrary connections and disconnections of nodes, due to several reasons (as hardware or software problems of the device). Notice that stationary nodes can only disconnect or connect, but they cannot move. Remaining rules are standard in process calculi.

The symbol $\longrightarrow^*$ denotes the reflexive and transitive closure of $\longrightarrow$, Figure 3 shows an example of observable action. Suppose that a node `n` (the red node

$$\text{(R-Bcast)}\ \frac{r \neq 0,\ \forall i \in I.d(l,l_i) \leq r,\ r_i \neq 0,\ |\tilde{x_i}| = |\tilde{v}|}{n[\bar{c}_{L,r}\langle\tilde{v}\rangle.P]^{\mu}_{l,r} \mid \prod_{i\in I} n_i[c(\tilde{x_i}).P_i]^{\mu_i}_{l_i,r_i} \rightarrow n[P]^{\mu}_{l,r} \mid \prod_{i\in I} n_i[P_i\{\tilde{v}/\tilde{x_i}\}]^{\mu_i}_{l_i,r_i}}$$

$$\text{(R-Rad)}\ \frac{r' \in [0,r_n]}{n[P]^{\mu}_{l,r} \rightarrow n[P]^{\mu}_{l,r'}} \qquad \text{(R-Move)}\ \frac{d(l,k) \leq \delta}{n[P]^{\mathtt{m}}_{l,r} \rightarrow n[P]^{\mathtt{m}}_{k,r}}$$

$$\text{(R-Par)}\ \frac{M \rightarrow M'}{M|N \rightarrow M'|N} \qquad \text{(R-Res)}\ \frac{M \rightarrow M'}{(\nu c)M \rightarrow (\nu c)M'}$$

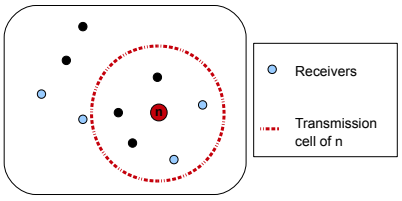
$$\text{(R-Struct)}\ \frac{M \equiv N\ N \rightarrow N'\ N' \equiv M'}{M \rightarrow M'}$$

Table 3: Reduction Semantics

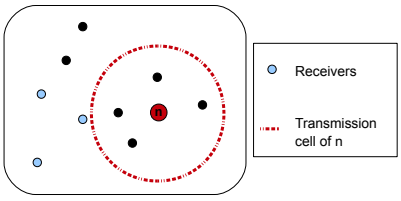
in figure) broadcasts a message to a set L of devices. Black nodes represent all the locations of the network not included in L, while light blue nodes represent locations in L, which are the real receivers of the message. Figure 3a models the case in which at least one of the locations in L lies in the transmission area of the sender, while Figure 3b models a *non-observable action*, where none of the locations in L is able to receive the message.

Fig. 3: Transmission observability

(a) Observable action



(b) Non-observable action



2.2 Behavioural Semantics

In operational semantics two terms are deemed equivalent if they have the same observational behaviour in all possible contexts. The central actions of the

calculus here proposed are input and output of a message, but only the output action is observable. An observer cannot be sure whether an intended receiver actually received a given value. Instead, if a node receives a message, then surely someone must have sent it (the network never invents messages!). Following Milner and Sangiorgi [22] we use the term *Barb* as a synonymous of observable. However our definition of barb, compared to the one proposed in [14] presents an important difference: a transmission is considered an observable action only if at least one location of the set of receivers is able to receive the message, in other words if a location in L associated to the channel c can receive the message transmitted.

Definition 1 (Barb). *Let* $M \equiv (\nu \tilde{d})(n[\bar{c}_{L,r}\langle \tilde{v} \rangle.P]^{\mu}_{l,r} | M')$, *with* $c \notin \tilde{d}$.
If $\exists k \in L \wedge d(l,k) \leqslant r$ *then* $M \downarrow_c$
If $M \longrightarrow^* M' \downarrow_c$ *then* $M \Downarrow_c$.

This definition ensures that, for a given process $M \equiv (\nu \tilde{d})(n[\bar{c}_{L,r}\langle \tilde{v} \rangle.P]^{\mu}_{l,r} | M')$, if $M \downarrow_c$, we can be sure that at least one of the recipients of the message $\tilde{v}$ is able to correctly listen to the transmission. This process will be in the form $N \equiv (\nu \tilde{d_i})(n_i[c(\tilde{x}).Q]^{\mu_i}_{l_i,r_i} | N')$, with $c \notin \tilde{d_i}$ and $l_i \in \{k : k \in L \wedge d(k,l) \leqslant r\}$.

Definition 2. *A relation* $\mathcal{R}$ *is* barb preserving *if* $M \mathcal{R} N$ *and* $M \downarrow_c$ *implies* $N \Downarrow_c$

Definition 3. *A relation* $\mathcal{R}$ *is* reduction closed *if* $M \mathcal{R} N$ *and* $M \longrightarrow M'$ *implies the existence of some* N' *such that* $N \longrightarrow^* N'$ *and* $M' \mathcal{R} N'$

Definition 4. *A relation* $\mathcal{R}$ *is* contextual *if* $M \mathcal{R} N$ *implies* $\mathcal{C}[M] \mathcal{R} \mathcal{C}[N]$ *for all contexts* $\mathcal{C}[\cdot]$.

Definition 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 LTS Semantics

In this section we describe the **LTS** semantics (*Label Transition System*) of E-BUM. LTS 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 $c\tilde{v}$ and $\bar{c}_{L,r}\tilde{v}$ denote, respectively, input and output of a tuple $\tilde{v}$ of values at channel c. The grammar for η is:

$$\eta ::= c\tilde{v} \mid \bar{c}_{L,r}\tilde{v}. \tag{2}$$

Rules for processes are simple and they not need deeper explanations.

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

$$\gamma ::= c?\tilde{v}@l \mid c_L!\tilde{v}[l,r] \mid c!\tilde{v}@K \mid \tau. \tag{3}$$

Rule (Snd) models the sending, with transmission radius r, of the tuple $\tilde{v}$ of values via channel c to the set L of receivers, while rule (Rcv) models the reception of $\tilde{v}$ at l via channel c. Rule (Bcast) models the propagation of broadcast. All the nodes lying within the transmission cell of the transmitter may hear the communication, regardless of the fact that the node hearing the communication is a member of L. Rule (Obs) models the observability of a transmission: every output action may be detected (and hence *observed*) by any receiver located within the transmission cell of the sender. The action $c!\tilde{v}@K$ represents the transmission of tuple $\tilde{v}$ of messages via c to the set of recipients of L whose locations lie within the transmission cell of the transmitter ($K = \{k : k \in L \wedge d(k,l) \leqslant r\}$ where l and r are respectively the location and the transmission radius of the message sender). If $K \neq \emptyset$ this is an observable action corresponding to the barb $\downarrow_c$. Rule (Lose) models both message loss and a local activity of the network which an observer is not party to. τ-actions are used, as commonly in process calculi, to denote non-observable actions. Rule (Move) models 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 (Rad) models the possibility for a node n to change its transmission radius, provided that is within $[0, r_n]$. This rule allows to represent also arbitrary connections and disconnections of a node (in particular a radius set to 0 represent a disconnected node). On end we prove that LTS-based semantics coincides with the reduction semantics and the notion of observability given in the previous section.

Lemma 1.

1. *If* $M \xrightarrow{c?\tilde{v}@l} M'$, *then there are* n, P, μ, l, r, M_1 *and* $\tilde{d}$, *with* $c \notin \tilde{d}$, *such that*

$$M \equiv (\nu\tilde{d})(n[c(\tilde{x}).P]^{\mu}_{l,r} | M_1)$$

and

$$M' \equiv (\nu\tilde{d})(n[\{\tilde{v}/\tilde{x}\}P]^{\mu}_{l,r} | M_1).$$

2. *If* $M \xrightarrow{c_L!\tilde{v}[l,r]} M'$, *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, l_i, r_i, *with* $d(l,l_i) \leq r$ *for all* $i \in I$, *such that:*

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

and

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

Proof. Proof can be obtained by induction on the transition rules of Table 5.
Case 1: $M \xrightarrow{c?\tilde{v}@l} M'$

(Rcv) Let $M \xrightarrow{c?\tilde{v}@l} M'$, then there exist n, P, μ such that $M \equiv n[P]^{\mu}_{l,r}$ and $M' \equiv n[P']^{\mu}_{l,r}|$. Since $P \xrightarrow{c\tilde{v}} P'$ then there must be Q such that
$P = c(\tilde{v}).Q$ and $P' = \{\tilde{v}/\tilde{x}\}Q$, then, if we suppose $\tilde{d}$ and M_1 empty, lemma is proved because
$M \equiv n[c(\tilde{v}).Q]^{\mu}_{l,r}$ and $M' \equiv n[\{\tilde{v}/\tilde{x}\}Q]^{\mu}_{l,r}$.

(Par) If $M|N \xrightarrow{c?\tilde{v}@l} M'|N$, then $M \xrightarrow{c?\tilde{v}@l} M'$. Then, by induction hypothesis we have $M \equiv (\nu\tilde{d})(n[c(\tilde{x}).P]^{\mu}_{l,r}|M_1)$ and $M' \equiv (\nu\tilde{d})(n[\{\tilde{v}/\tilde{x}\}P]^{\mu}_{l,r}|M_1)$. Since $\tilde{d}$ is a tuple of new names in M, they can be chosen so that they are new also for N (we consider in this calculus the equivalence with respect to α-conversion). Then, since by hypothesis $c \notin \tilde{d}$, by applying rule (Struct-Res-Par) of structural congruence we can write:
$M|N \equiv (\nu\tilde{d})(n[c(\tilde{x}).P]^{\mu}_{l,r}|M_1|N)$ and $M'|N \equiv (\nu\tilde{d})(n[\{\tilde{v}/\tilde{x}\}P]^{\mu}_{l,r}|M_1|N)$.

(Res) Suppose $(\nu d')M \xrightarrow{c?\tilde{v}@l} (\nu d')M'$, then $M \xrightarrow{c?\tilde{v}@l} M'$. Then, by induction hypothesis $M \equiv (\nu\tilde{d})(n[c(\tilde{x}).P]^{\mu}_{l,r}|M_1)$ and $M' \equiv (\nu\tilde{d})(n[\{\tilde{v}/\tilde{x}\}P]^{\mu}_{l,r}|M_1)$. Since by hypothesis $d' \notin fc(c?\tilde{v}@l)$ then $c \neq d'$. Since $\tilde{d''} = \tilde{d} \bigcup \{d'\}$, then we can write:
$(\nu d')M \equiv (\nu\tilde{d''})(n[c(\tilde{x}).P]^{\mu}_{l,r}|M_1)$ and $(\nu d')M' \equiv (\nu\tilde{d''})(n[\{\tilde{v}/\tilde{x}\}P]^{\mu}_{l,r}|M_1)$.
The other cases follow straightforwardly from congruence rules of the reduction relation.

Case 2: $M \xrightarrow{c_L!\tilde{v}[l,r]} M'$

(Snd) Let $M \xrightarrow{c_L!\tilde{v}[l,r]} M'$, then there exist n, P, μ such that $M \equiv n[P]^{\mu}_{l,r}$. Since $P \xrightarrow{c_{\bar{L},r}\tilde{v}} P'$, then there must be Q such that
$P = \bar{c}_{L,r}\langle\tilde{v}\rangle.Q$ and $P' = Q$, then, if we suppose $\tilde{d}$ and M_1 empty, lemma is proved because
$M \equiv (\nu\tilde{d})(n[\bar{c}_{L,r}\langle\tilde{v}\rangle.P]^{\mu}_{l,r}|M_1)$ and $M' \equiv (\nu\tilde{d})(n[P]^{\mu}_{l,r}|M_1)$

(Bcast) Let $M|N \xrightarrow{c_L!\tilde{v}[l,r]} M'|N'$ because $M \xrightarrow{c_L!\tilde{v}[l,r]} M'$ and $N \xrightarrow{c?\tilde{v}@l'} N'$, with $d(l,l') \leq r$. By induction hypothesis:

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

and

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

for some 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, l_i, r_i, with $d(l,l_i) \leq r$ for all $i \in I$, and

$$N \equiv (\nu\tilde{d'})(n'[c(\tilde{x}).Q]^{\mu'}_{l',r'}|N_1)$$

and

$$N' \equiv (\nu\tilde{d'})(n'[\{\tilde{v}/\tilde{x}\}Q]^{\mu'}_{l',r'}|N_1).$$

for some n', Q, μ', l', r', N_1 and $\tilde{d'}$, with $c \notin \tilde{d'}$

then we can write:

$$M|N \equiv (\nu \tilde{d''})(n[\bar{c}_{L,r}\langle \tilde{v} \rangle.P]^{\mu}_{l,r} | \prod_{i \in I} n_i[c(\tilde{x_i}).P_i]^{\mu_i}_{l_i,r_i} | n'[c(\tilde{x}).Q]^{\mu'}_{l',r'} | M_1 | N_1)$$

and

$$M'|N' \equiv (\nu \tilde{d''})(n[P]^{\mu}_{l,r} | \prod_{i \in I} n_i[\{\tilde{v}/\tilde{x_i}\}P_i]^{\mu_i}_{l_i,r_i} | n'[\{\tilde{v}/\tilde{x}\}Q]^{\mu'}_{l',r'} | M_1 | N_1).$$

with $\tilde{d''} = \tilde{d} \cup \tilde{d'}$ Proof of the other cases is analogous to the first part of the lemma.

Lemma 2 ($\equiv$ respects transitions). *If $M \xrightarrow{\gamma} M'$ and $M \equiv N$ then there exists N' such that $N \xrightarrow{\gamma} N'$ and $M' \equiv N'$*

Proof. Proof proceeds by induction on the depth of the inference $M \longrightarrow M'$. The full proof must treat all possible cases for the final step of the inference $M \xrightarrow{\gamma} M'$. Here we consider just some cases.

(Par) Suppose $M|N \xrightarrow{\gamma} M'|N$, inferred by rule (Par), where $M \xrightarrow{\gamma} M'$; Many are the possible structural congruence rules to apply. For example we can consider the rule (Struct Par Comm), then if $M|N \equiv N|M$, by applying (Par) we obtain $N|M \xrightarrow{\gamma} N|M'$, and, by applying (Struct Par Comm) we finally obtain $N|M' \equiv M'|N$. Considering rule (Struct Cxt Par), if $M_1 \equiv M$ and $Q = M_1|N$, then, for induction hypothesis $M \xrightarrow{\gamma} M'$ and $M \equiv M_1$ implies $M_1 \xrightarrow{\gamma} M_1'$ and $M' \equiv M_1'$. We can so deduce $M_1|N \xrightarrow{\gamma} M_1'|N$ and $M'|N \equiv M_1'|N$, by using the rule (Struct Cxt Par).

(Res) Suppose $(\nu c)M \xrightarrow{\gamma} (\nu c)M'$, inferred by $M \xrightarrow{\gamma} M'$ (with $c \notin fc(\gamma)$); now there are many ways in which $(\nu c)M \equiv Q$ due to a single use of a structural congruence rule; we will confine ourselves to considering just some cases.
If $M \equiv N$ for some N, using the rule (Struct Cxt Res) we deduce $(\nu c)M \equiv (\nu c)N$. By induction hypothesis, since $M \xrightarrow{\gamma} M'$ and $M \equiv N$, then there exists N' such that $N \xrightarrow{\gamma} N'$ and $M' \equiv N'$. Using the rule (Res) in $N \xrightarrow{\gamma} N'$, considering that $c \notin fc(\gamma)$, we obtain $(\nu c)N \xrightarrow{\gamma} (\nu c)N'$. Finally, by applying again the rule (Struct Cxt Res) to $M' \equiv N'$ we obtain $(\nu c)M' \equiv (\nu c)N'$.

The other cases are proved in analogous way.

Theorem 1 (Harmony theorem).

1. *$M \downarrow_c$ iff $M \xrightarrow{c!\tilde{v}@K}$ for some value $\tilde{v}$ and some set K of locations.*
2. *If $M \xrightarrow{\tau} M'$ then $M \longrightarrow M'$.*
3. *If $M \longrightarrow M'$ then $M \xrightarrow{\tau} \equiv M'$.*

Proof.
1. The first part follows from definition of barb and from Lemma 1.

2. The second part is proved by induction on the derivation $M \xrightarrow{\tau} M'$.
Suppose that the τ-action has been generated by an application of the rule (Lose). In this case we have $\dfrac{M \xrightarrow{c_L!\tilde{v}[l,r]} M'}{M \xrightarrow{\tau} M'}$, then, by an application of Lemma 1 we have:

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

and

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

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

$$(\nu\tilde{d})(n[\bar{c}_{L,r}\langle\tilde{v}\rangle.P]^{\mu}_{l,r} | \prod_{i\in I} n_i[c(\tilde{x}).P_i]^{\mu_i}_{l_i,r_i} | M_1) \longrightarrow (\nu\tilde{d})(n[P]^{\mu}_{l,r} | \prod_{i\in I} n_i[\{\tilde{v}/\tilde{x_i}\}P_i]^{\mu_i}_{l_i,r_i} | M_1)$$

and, by applying (R-Struct), we obtain $M \longrightarrow M'$, as required. Suppose now that the τ-action has been generated by an application of rule (Move):

$$\frac{d(k,l) \leq r}{n[P]^{\mathtt{m}}_{l,r} \xrightarrow{\tau} n[P]^{\mathtt{m}}_{k,r}}$$

then, by an application of (R-Move) we get

$$\frac{d(k,l) \leq r}{n[P]^{\mathtt{m}}_{l,r} \longrightarrow n[P]^{\mathtt{m}}_{k,r}}.$$

The other cases, as the rule (Move), follow straightforwardly from congruence rules of the reduction relation.

3. The third part of the theorem is proved by induction on the derivation $M \rightarrow M'$. If we consider the rules where a τ-action in LTS semantics corresponds to a reduction (for example (Move) and (R-Move)), proof can be omitted. We're going to describe the other cases.
Suppose that the derivation $M \longrightarrow M'$ has been generated by an application of rule (R-Bcast)

$$\frac{r \neq 0 \, \forall i \in I . d(l, l_i) \leq r \wedge r_i \neq 0}{n[\bar{c}_{L,r}\langle\tilde{v}\rangle.P]^{\mu}_{l,r} | \prod_{i\in I} n_i[c(\tilde{x_i}).P_i]^{\mu_i}_{l_i,r_i} \rightarrow n[P]^{\mu}_{l,r} | \prod_{i\in I} n_i[\{\tilde{v}/\tilde{x_i}\}P_i]^{\mu_i}_{l_i,r_i}}$$

Then, by applying rules (Snd), (Rcv) and (Bcast) we obtain:

$$\frac{\dfrac{\bar{c}_{L,r}\langle\tilde{v}\rangle.P \xrightarrow{\bar{c}_{L,r}\tilde{v}} P \; r \neq 0}{n[\bar{c}_{L,r}\langle\tilde{v}\rangle.P]^{\mu}_{l,r} \xrightarrow{c_L!\tilde{v}[l,r]} n[P]^{\mu}_{l,r}} \quad \dfrac{c(\tilde{x_1}).P_1 \xrightarrow{c\tilde{v}} \{\tilde{v}/\tilde{x_1}\}.P_1 \; r_1 \neq 0}{n_1[c(\tilde{x_1}).P_1]^{\mu_1}_{l_1,r_1} \xrightarrow{c?\tilde{v}@l_1} n_1[\{\tilde{v}/\tilde{x_1}\}P_1]^{\mu_1}_{l_1,r_1}} \; d(l,l_1) \leq r}{n[\bar{c}_{L,r}\langle\tilde{v}\rangle.P]^{\mu}_{l,r} | n_1[c(\tilde{x_1}).P_1]^{\mu_1}_{l_1,r_1} \xrightarrow{c_L!\tilde{v}[l,r]} n[P]^{\mu}_{l,r} | n_1[\{\tilde{v}/\tilde{x_1}\}P_1]^{\mu_1}_{l_1,r_1}}.$$

Table 4: **LTS**-Processes

$$\text{(Input)}\ \frac{-}{c(\tilde{x}).P \xrightarrow{c\tilde{v}} \{\tilde{v}/\tilde{x}\}P} \qquad \text{(Output)}\ \frac{-}{\bar{c}_{L,r}\langle\tilde{v}\rangle.P \xrightarrow{\bar{c}_{L,r}\tilde{v}} P}$$

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

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

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

$$n[\bar{c}_{L,r}\langle\tilde{v}\rangle.P]^{\mu}_{l,r} | \prod_{i\in I} n_i[c(\tilde{x_i}).P_i]^{\mu_i}_{l_i,r_i} \xrightarrow{\tau} n[P]^{\mu}_{l,r} | \prod_{i\in I} n_i[\{\tilde{v}/\tilde{x_i}\}P_i]^{\mu_i}_{l_i,r_i}$$

as required. Suppose that the derivation $M \longrightarrow M'$ has been generated by an application of rule (R-Struct)

$$\frac{M \equiv N\ N \rightarrow N'\ N' \equiv M'}{M \rightarrow M'}$$

By induction hypothesis $N \xrightarrow{\tau} \equiv N'$, then there exists N'' such that $N \xrightarrow{\tau} N''$ and $N'' \equiv N'$. Then, using Lemma 2 there exists M'' such that $M \xrightarrow{\tau} \equiv M''$ and $M'' \equiv N''$. By transitivity of $\equiv$ it follows that $M'' \equiv M'$, then $M \xrightarrow{\tau} \equiv M'$ as required. Finally, as both the τ-transitions and structural congruence are preserved by network contexts, the cases when the reduction $M \longrightarrow M'$ is derived either by rules (R-Par) or rule (R-res) are straightforward.

4 Simulation and Bisimulation

In this section, using our LTS, we define notions of simulation and bisimulation. Then we prove that bisimulation is a complete characterisation of *reduction barbed congruence*, and hence represents a valid method for proving that two networks are reduction barbed congruent. This property let us deal with all issues that do not permit the correct behaviour of mobile ad hoc networks. We then have to prove both that $\cong \subseteq \approx$ and that $\approx \subseteq \cong$.

For convenience we use metavariable α to range over those actions that will be used in the definition of bisimulation.

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

Since we are interested in *weak behavioural equivalences*, that abstract over τ-actions, we introduce the notion of *weak action*.

Table 5: **LTS**-Networks

$$\text{(Snd)}\ \frac{P \xrightarrow{\bar{c}_{L,r}\tilde{v}} P'}{n[P]^{\mu}_{l,r} \xrightarrow{c_L!\tilde{v}[l,r]} n[P']^{\mu}_{l,r}}\, r \neq 0 \qquad \text{(Rcv)}\ \frac{P \xrightarrow{c\tilde{v}} P'}{n[P]^{\mu}_{l,r} \xrightarrow{c?\tilde{v}@l} n[P']^{\mu}_{l,r}}\, r \neq 0$$

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

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

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

$$\text{(Rad)}\ \frac{r' \in [0, r_n]}{n[P]^{\mu}_{l,r} \xrightarrow{\tau} n[P]^{\mu}_{l,r'}}$$

$$\text{(Par)}\ \frac{M \xrightarrow{\gamma} M'}{\begin{array}{c} M|N \xrightarrow{\gamma} M'|N \\ N|M \xrightarrow{\gamma} N|M' \end{array}} \qquad \text{(Res)}\ \frac{M \xrightarrow{\gamma} M'\ c \notin fc(\gamma)}{(\nu c)M \xrightarrow{\gamma} (\nu c)M'}$$

- $\Rightarrow$ denotes reflexive and transitive closure of $\xrightarrow{\tau}$
- $\overset{c?\tilde{v}@F}{\Longrightarrow}$ denotes $\Rightarrow \xrightarrow{c?\tilde{v}@l_1} \Rightarrow \ldots \Rightarrow \xrightarrow{c?\tilde{v}@l_n} \Rightarrow$ for $F = \{l_1, ..., l_n\}$
- $\overset{c!\tilde{v}@K}{\Longrightarrow}$ denotes $\overset{c?\tilde{v}@F_1}{\Longrightarrow} \xrightarrow{c!\tilde{v}@K_1} \overset{c?\tilde{v}@F'_1}{\Longrightarrow} \ldots \overset{c?\tilde{v}@F_n}{\Longrightarrow} \xrightarrow{c!\tilde{v}@K_n} \overset{c?\tilde{v}@F'_n}{\Longrightarrow}$, for $\bigcup_{i=1}^{n} K_i = K, \bigcup_{j=1}^{n}(F_1 \cup F'_1) = F \wedge F \cap K = \emptyset$;
- $\overset{\hat{\alpha}}{\Longrightarrow}$ denotes $\Rightarrow$ if $\alpha = \tau$ and $\overset{\alpha}{\Longrightarrow}$ otherwise;

Notice that the third point of this definition means that a distributed observer receiving an instance of message $\tilde{v}$, at each location in K, in several computational steps, cannot assume that those messages belong to the same broadcast transmission, but they may be different transmissions of the same message. The presence of the weak input actions are due to the fact that we want to ignore all the input executed by each location which is not included in the set of receivers. Let understand with a little example the importance of abstract from this type of input actions.

Example 1. Let M be a process such that

$$M \xrightarrow{c!\tilde{v}@K} M' \text{ because } M \xrightarrow{c_L!\tilde{v}[l,r]} M' \ .$$

Then

$$\forall l' \notin K \; M|n[c(\tilde{x}).P]^{\mu}_{l',r'} \stackrel{c!\tilde{v}@K}{\Longrightarrow} M|n[\{\tilde{v}/\tilde{x}\}P]^{\mu}_{l',r'}.$$

In other words if a node sends a message to a given set L of receivers, we will not mind if other nodes, lying at some location not included in L and listening to channel c, can perform a synchronisation with the node having sent the message or they do not.

Definition 6 (Bisimilarity). *A binary relation $\mathcal{R}$ over networks is a* simulation *if $M\mathcal{R}N$ implies:*

- *If $M \xrightarrow{\alpha} M'$, $\alpha \neq c?\tilde{v}@l$, then there exists N' such that $N \stackrel{\hat{\alpha}}{\Longrightarrow} N'$ and $M'\mathcal{R}N'$*
- *If $M \xrightarrow{c?\tilde{v}@l} M'$ then there exists N' such that:*
  - *$N \stackrel{c?\tilde{v}@l}{\Longrightarrow} N'$ 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 a* bisimulation *if both $\mathcal{R}$ and its converse are simulations. We say that M and N are bisimilar, written $M \approx N$, if there exists some bisimulation $\mathcal{R}$ such that $M\mathcal{R}N$.*

It is easy now to prove that bisimulation is an equivalence relation, because reflexivity and symmetry are trivial, and transitivity follows from definition of $\stackrel{\hat{\alpha}}{\Longrightarrow}$. Notice that there are other important properties of bisimulation, here we will prove closure under contexts.

Lemma 3 ($\approx$ is contextual). *Let M and N be two networks such that $M \approx N$, then:*

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

Proof. As regards the first item we have to prove that the relation

$$\mathcal{S} = \{(M|O, N|O) \mid \forall O, M \approx N\}$$

is a bisimulation. To prove it we do a case analysis on the transition $M|O \xrightarrow{\alpha} \hat{M}$. The interesting cases are when the transition is due to an interaction between M and O, and this happens by an application of rule (Bcast). Let $M|O \xrightarrow{c!\tilde{v}@K} \hat{M}$ because $M|O \xrightarrow{c_L!\tilde{v}[l,r]} \hat{M}$ for some r, l, with $k \in L \wedge d(l,k) \leq r$, $\forall k \in K$, due to an application of (Bcast). There are then two possibilities:

1. $M|O \xrightarrow{c_L!\tilde{v}[l,r]} \hat{M}$ because $M \xrightarrow{c_L!\tilde{v}[l,r]} M'$ and $O \xrightarrow{c?\tilde{v}@l'} O'$ with $d(l,l') \leq r$ and $\hat{M} = M'|O'$
2. $M|O \xrightarrow{c_L!\tilde{v}[l,r]} \hat{M}$ because $M \xrightarrow{c?\tilde{v}@l'} M'$ and $O \xrightarrow{c_L!\tilde{v}[l,r]} O'$, with $d(l,l') \leq r$ and $\hat{M} = M'|O'$

Case 1. Now we have to consider two different cases, that depend by the presence or the absence of l' in the set L of receivers.

- If $l' \in L$, by an application of rule (Obs) $M \xrightarrow{c!\tilde{v}@K'} M'$, with $K' = K \cup \{l'\}$. As $M \approx N$ then there exists N' such that $N \overset{c!\tilde{v}@K'}{\Longrightarrow} N'$ with $M' \approx N'$. By applying rule (Obs) backward there must be $K_1, ..., K_n$ such that

$$N \Rightarrow \xrightarrow{c!\tilde{v}@K_1} ... \xrightarrow{c!\tilde{v}@K_n} \Rightarrow N'$$

with $\bigcup_{i=1}^{n} K_i = K'$ and $l' \in K_j$ for some $1 \leq k \leq n$. This implies

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

with $l_j \in L \wedge d(l_j, k) \leq r_j \; \forall k \in K_j$. Hence we can apply rule (Bcast):

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

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

- If $l' \notin L$, as $M \xrightarrow{c_L!\tilde{v}[l,r]} M'$, by applying rule (Par) we have $M|O \xrightarrow{c_L!\tilde{v}[l,r]} M'|O$, and, as $O \xrightarrow{c?\tilde{v}@l'} O'$, by applying again rule (Par) we obtain $M'|O \xrightarrow{c?\tilde{v}@l'} M'|O'$. As $M \approx N$ we can that $N \overset{c!\tilde{v}@K}{\Longrightarrow} N'$, and we can apply again rule (Par) obtaining $N|O \overset{c!\tilde{v}@K}{\Longrightarrow} N'|O$, and then $N'|O \xrightarrow{c?\tilde{v}@l'} N'|O'$. As $l' \notin K$ we deduce finally $N|O \overset{c!\tilde{v}@K}{\Longrightarrow} N'|O'$ as required.
  Case 2 $M|O \xrightarrow{c_L!\tilde{v}[l,r]} \hat{M}$ because $M \xrightarrow{c?\tilde{v}@l'} M'$ and $O \xrightarrow{c_L!\tilde{v}[l,r]} O'$, with $d(l, l') \leq r$ and $\hat{M} = M'|O'$. As $M \approx N$ then there exists N' such that:
  - $N \overset{c?\tilde{v}@l'}{\Longrightarrow} N'$, with $M' \approx N'$; in this case
    $$N|O \Rightarrow \xrightarrow{c_L!\tilde{v}[l,r]} \Rightarrow N'|O'$$
    and, by an application of rule (Obs), also $N|O \overset{c!\tilde{v}@K}{\Longrightarrow} N'|O'$, with $(M'|O', N'|O') \in \mathcal{S}$, as required.
  - or $N \Longrightarrow N'$, with $M' \approx N'$; in this case by applying rule (Par) we obtain
    $$N|O \Rightarrow \xrightarrow{c_L!\tilde{v}[l,r]} \Rightarrow N'|O'$$
    and, by applying rule (Obs) also $N|O \overset{c!\tilde{v}@K}{\Longrightarrow} N'|O'$, with $(M'|O', N'|O') \in \mathcal{S}$, as required.

Cases where there is no interaction between M and O are easy to deal with. In order to prove the second item of the lemma it suffices to show that the relation

$$\mathcal{S} \overset{\text{def}}{=} \{((\nu c)M, (\nu c)N) : M \approx N, \forall c\}$$

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, hence there is no *scope extrusion*.

We can now demonstrate that our bisimulation is a valid proof method for *reduction barbed congruence*.

Theorem 2 (Soundness). *Let M and N be two arbitrary networks, such that $M \approx N$. Then $M \cong N$*

Proof. By *Harmony theorem* we prove that bisimulation is reduction closed (items 2 and 3) and barb preserving (item 1), and by Lemma 3 we prove that bisimulation is contextual, thus $\approx \subseteq \cong$.

By Soundness theorem let us prove that bisimulation is a complete characterisation of *Reduction Barbed Congruence*, we are going now to prove that *Reduction Barbed Congruence* is a complete characterisation of bisimulation.

Proposition 1. *If $M \cong N$ then*

- *$M \Downarrow_c$ iff $N \Downarrow_c$*
- *$M \Longrightarrow M'$ implies that there is N' such that $N \Longrightarrow N'$ and $M' \cong N'$*

Lemma 4 (Completeness). *Let M and N be two arbitrary networks, such that $M \cong N$. Then $M \approx N$*

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

- Suppose that $M \mathcal{R} N$ and $M \xrightarrow{\tau} M'$. By applying harmony theorem $M \rightarrow M'$. Then there is N' such that $N \rightarrow^* N'$, hence $N \Longrightarrow N'$.
- Suppose $M \mathcal{R} N$ and $M \xrightarrow{c!\tilde{v}@K} M'$, with $K = \{k_1, ..., k_n\}$. As the action $c!\tilde{v}@K$ can only be generated by an application of rule (Obs), it follows that $M \xrightarrow{c_L!\tilde{v}[l,r]} M'$ for some l, r such that $k \in L \wedge d(l,k) \leq r \; \forall k \in K$. Let us build 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 $\mathcal{C}[\cdot] \stackrel{\text{def}}{=} [\cdot] \mid \prod_{i=1}^{n}(m_i[c(\tilde{x}).[\tilde{x} = \tilde{v}]\bar{\mathtt{f}}^{(i)}_{\infty,r_i}\langle\tilde{x}\rangle]^{\mathtt{s}}_{k_i,r_i} \mid n_i[\mathtt{f}^{(i)}(\tilde{x}).\bar{\mathtt{ok}}^{(i)}_{\infty,r_i}\langle\tilde{x}\rangle]^{\mathtt{s}}_{k_i,r_i})$ with names m_i, n_i for $1 \leq i \leq n$ and channels names $\mathtt{f}^{(i)}$, $\mathtt{ok}^{(i)}$ for $1 \leq i \leq n$ fresh. Intuitively, the existence of the barbs on the fresh channels $\mathtt{f}^{(i)}$ indicates that the action has not yet happened, whereas the presence of the barbs on channels $\mathtt{ok}^{(i)}$, together with the absence of the barbs on channels $\mathtt{f}^{(i)}$ ensures that the action has been performed.
  As $\cong$ is preserved by network contexts, $M \cong N$ implies $\mathcal{C}[M] \cong \mathcal{C}[N]$. As $M \xrightarrow{c_L!\tilde{v}[l,r]} M'$ it follows that
  $\mathcal{C}[M] \Longrightarrow M' | \prod_{i=1}^{n}(m_i[\mathbf{0}]^{\mathtt{s}}_{k_i,r_i} | n_i[\bar{\mathtt{ok}}^{(i)}_{\infty,r_i}\langle\tilde{x}\rangle]^{\mathtt{s}}_{k_i,r_i}) = \hat{M}$, with $\hat{M} \not\Downarrow_{\mathtt{f}^{(i)}}$ and $\hat{M} \Downarrow_{\mathtt{ok}^{(i)}}$, for $1 \leq i \leq n$.
  The reduction sequence must be matched by a corresponding reduction sequence $\mathcal{C}[N] \Longrightarrow \hat{N}$ with $\hat{M} \cong \hat{N}$, $\hat{N} \not\Downarrow_{\mathtt{f}^{(i)}}$ and $\hat{N} \Downarrow_{\mathtt{ok}^{(i)}}$ for $1 \leq i \leq n$. The constrains on the barbs allow us to deduce the structure of the above reduction sequence

$\mathcal{C}[N] \Longrightarrow N' | \prod_{i=1}^{n} (m_i[\mathbf{0}]^{\mathtt{s}}_{k_i,r_i} | n_i[\bar{\mathtt{ok}}^{(i)}_{\infty,r_i}\langle\tilde{x}\rangle]^{\mathtt{s}}_{k_i,r_i}) = \hat{N}$.

This implies $N \stackrel{c!\tilde{v}@K'}{\Longrightarrow} N'$ with $K \subseteq K'$. More precisely, the derivative N' might be reached performing several outputs of the message $\tilde{v}$ along the same channel c. We can prove that K' contains K because we are sure that all nodes m_i hare reached by a transmission along channel c from N. it is easy now to show that $N \stackrel{c!\tilde{v}@K}{\Longrightarrow} N'$, by considering in the composition of the action only on those outputs addressed to the locations in K, and turning the other in τ-actions, using rule (Lose).

As $\hat{M} \cong \hat{N}$, and as Reduction Barbed Congruence is preserved by restriction, we have $(\nu \mathtt{f}, \mathtt{ok})\hat{M} \cong (\nu \mathtt{f}, \mathtt{ok})\hat{N}$. As $\mathtt{f}^{(i)}$ and $\mathtt{ok}^{(i)}$ for all $1 \leq i \leq n$ fresh, by applying structural congruence we have

$(\nu \mathtt{f}, \mathtt{ok})\hat{M} \equiv M' | (\nu \mathtt{f}, \mathtt{ok})(m_i[\mathbf{0}]^{\mathtt{s}}_{k_i,r_i} | n_i[\bar{\mathtt{ok}}^{(i)}_{\infty,r_i}\langle\tilde{x}\rangle]^{\mathtt{s}}_{k_i,r_i})$

$(\nu \mathtt{f}, \mathtt{ok})\hat{N} \equiv N' | (\nu \mathtt{f}, \mathtt{ok})(m_i[\mathbf{0}]^{\mathtt{s}}_{k_i,r_i} | n_i[\bar{\mathtt{ok}}^{(i)}_{\infty,r_i}\langle\tilde{x}\rangle]^{\mathtt{s}}_{k_i,r_i})$.

Using bisimilarity definition and soundness theorem we can easily prove that $(\nu \mathtt{f}, \mathtt{ok})(m_i[\mathbf{0}]^{\mathtt{s}}_{k_i,r_i} | n_i[\bar{\mathtt{ok}}^{(i)}_{\infty,r_i}\langle\tilde{x}\rangle]^{\mathtt{s}}_{k_i,r_i}) \cong \mathbf{0}$.

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

– Suppose that $M \mathcal{R} N$ and $M \xrightarrow{c?\tilde{v}@l} M'$.

The reception of a message cannot be directly observed. So we have to build a context which let the action be observable.

A context associated to the action $M \xrightarrow{c?\tilde{v}@l} M'$ could be:

$\mathcal{C}[\cdot] \stackrel{\text{def}}{=} [\cdot] | n[\bar{c}_{l,r}\langle\tilde{v}\rangle.\bar{\mathtt{f}}_{\infty,r}\langle\tilde{v}\rangle.\bar{\mathtt{ok}}_{\infty,r}\langle\tilde{v}\rangle]^{\mathtt{s}}_{k,r}$

with $\mathtt{f}$ and $\mathtt{ok}$ fresh channels, and $d(l,k) \leq r$. As $\cong$ is preserved by network contexts, $\mathcal{C}[M] \cong \mathcal{C}[N]$. As $M \xrightarrow{c?\tilde{v}@l} M'$ it follows that

$\mathcal{C}[M] \Longrightarrow M' | n[\bar{\mathtt{ok}}_{\infty,r}\langle\tilde{v}\rangle]^{\mathtt{s}}_{k,r} = \hat{M}$

with $\hat{M} \not\Downarrow_{\mathtt{f}}$ and $\hat{M} \Downarrow_{\mathtt{ok}}$. The reduction sequence must be matched by a corresponding reduction sequence $\mathcal{C}[N]$, so we have $\mathcal{C}[N] \Longrightarrow \hat{N}$ and $\hat{M} \cong \hat{N}$, with $N \not\Downarrow_{\mathtt{f}}$ and $N \Downarrow_{\mathtt{ok}}$. The constrains on the barb ensure that the action $c?\tilde{v}@l$ has been performed, so there exists N' such that $N \stackrel{c?\tilde{v}@l}{\Longrightarrow} N'$, or $N \Longrightarrow N'$, in case rule (Lose) has been applied to the node n. As $\hat{M} \cong \hat{N}$, and $\cong$ is preserved by restriction, it follows that $(\nu \mathtt{ok})\hat{M} \cong (\nu \mathtt{ok})\hat{N}$, from which we can easily derive

$(\nu \mathtt{ok})\hat{M} \equiv M' | (\nu \mathtt{ok})(n[\bar{\mathtt{ok}}_{\infty,r}\langle\tilde{v}\rangle]^{\mathtt{s}}_{k,r})$

$(\nu \mathtt{ok})\hat{N} \equiv N' | (\nu \mathtt{ok})(n[\bar{\mathtt{ok}}_{\infty,r}\langle\tilde{v}\rangle]^{\mathtt{s}}_{k,r})$

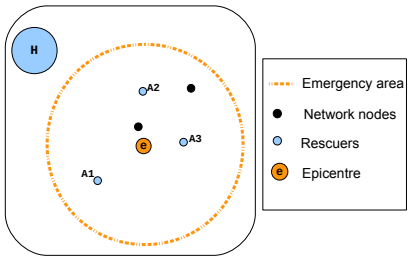
As $(\nu \mathtt{ok})(n[\bar{\mathtt{ok}}_{\infty,r}\langle\tilde{v}\rangle]^{\mathtt{s}}_{k,r}) \equiv \mathbf{0}$ we obtain $M' \cong N'$, as required.

We have proved that $\cong \subseteq \approx$.

5 Properties

In this section we use E-BUM to define and prove some properties of mobile ad hoc networks. First we review the properties for MANETs described in [14] and then we study some new properties which cannot be dealt with in the original CMN model. We use some examples to better describe the properties

Fig. 4: Installation of a mobile Ad-Hoc network after an earthquake



analysed. We use a running example depicted in Figure 4, describing the case of an emergency due to an earthquake. The hospital sends three ambulances to the emergency area (in figure A1, A2, A3). Then an ad hoc network is installed to manage the communication between the ambulances, placing a router near the epicentre of the earthquake. (in figure the orange circle).

We have to make an assumption before starting to deal with the properties of E-BUM, about the possible receivers of the whole set of transmissions of a network. Given a process P, we denote by $\mathtt{rcv}(P)$ the minimum set of locations ensuring that for each output action $\bar{c}_{L,r}\langle\tilde{v}\rangle$ performed by P it holds that $L \subseteq \mathtt{rcv}(P)$. Indeed, the tag L associated to an output action occurring in P can be either a variable or a set of locations, then we are not able to statically calculate $\mathtt{rcv}(P)$. However. since an ad hoc network is usually designed to guarantee the communications within a specific area, we can reasonably assume that the underling protocol will always multicast messages to recipients located within the interested area and we can abstractly represent them by a finite set of locations.

5.1 Ubiquity of nodes

We now provide to demonstrate that the position of a node in the network has no effect on its behaviour. This characteristic allows us to consider movements, connections and disconnections of the nodes as weak actions, and give us insights on how to analyse the problem of *Location Confidentiality*, because a node can hide information about its location without modifying the process it is executing. This property is important especially in those cases where confidentiality is a critical information to protect: the best example is in case of war. In our example the ubiquity of nodes ensures that communication between ambulances is not compromised by arbitrary movements of the nodes within the transmission cell of the router.

Theorem 3 (Ubiquity of nodes). *Let P be a process, l_1, l_2 locations r_1, r_2 a transmission radii. Then:*

1. $n[P]^{\mathtt{m}}_{l_1,r_1} \approx n[P]^{\mathtt{m}}_{l_2,r_2}$

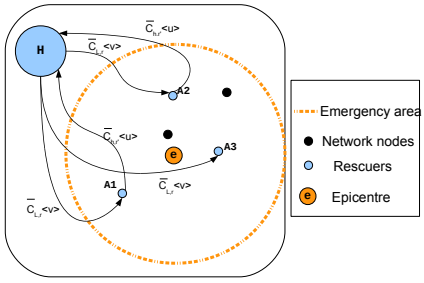
2. $n[P]^{\mathtt{s}}_{k,r_1} \approx n[P]^{\mathtt{s}}_{k,r_2}$

Proof.

1. We show that
   $\mathcal{S} = \{(n[P]^{\mathtt{m}}_{l_1,r_1}, n[P]^{\mathtt{m}}_{l_2,r_2}) : \forall P, l_1, l_2, r_1, r_2\} \bigcup \mathcal{I}$
   is a bisimulation (where $\mathcal{I}$ is the identity relation). It is easy to prove because, if for some α we have
   $$n[P]^{\mathtt{m}}_{l_1,r_1} \xrightarrow{\alpha} M,$$
   then, by applying rule (Move) and(Rad) in order to place n at location l_2 and to adjust its radius according with the protocol executed, we obtain
   $$n[P]^{\mathtt{m}}_{l_2,r_2} \stackrel{\hat{\alpha}}{\Longrightarrow} M.$$
2. We prove that
   $\mathcal{S} = \{(n[P]^{\mathtt{s}}_{k,r_1}, n[P]^{\mathtt{s}}_{k,r_2}) : \forall P, k, r_1, r_2\} \bigcup \mathcal{I}$
   is a bisimulation (where $\mathcal{I}$ is the identity relation). Suppose, for any α
   $$n[P]^{\mathtt{s}}_{k,r_1} \xrightarrow{\alpha} M,$$
   then, by applying (Rad) we obtain
   $$n[P]^{\mathtt{s}}_{k,r_2} \stackrel{\hat{\alpha}}{\Longrightarrow} M.$$

5.2 Silent nodes cannot be observed

Fig. 5: Messages exchange between H and the ambulances



What is interesting about the ad hoc networks are the interactions between nodes. If a node sends no messages, it does not interact with the network, then an external observer cannot know if this node is connected. Consider now the interactions between the hospital and the ambulances (Figure 5). Suppose that A1 and A2 are facing critical situations, and communicate with the hospital to prepare the acceptance of patients in hospital, while A3 have no patients

to be accepted so no communications are sent from A3 to the hospital. The hospital broadcasts emergency messages to update the network about the general situation. An observer listening the communication between the nodes cannot know if A3 is connected, because it does not receive anything from that node.

Theorem 4 (Silent nodes are not observable). *If the process P does not contain output constructs, then*
$n[P]^{\mu}_{l,r} \approx \mathbf{0}\ \forall \mu, l, r.$

Proof. It follows from the definition of bisimilarity in which it is possible to match both τ-actions and input actions with weak τ-actions.

5.3 Obfuscating message transmission

We are going to propose a way to obfuscate messages transmission. This property is very important to reason about security problems and information and location confidentiality. We first have to prove that, alternating infinite output sequences, the order of the transmissions has got no effect to the behaviour of the node. We prove the theorem for a set of two messages (u and v), but the result can be generalised to an arbitrary set $V = \{v_1, ..., v_n\}$ of messages.

Theorem 5 (Mixing up infinite output sequences). *Let*
$ALT(a, L_1, r_1, b, L_2, r_2) \stackrel{\text{def}}{=} \bar{c}_{L_1,r_1}\langle a\rangle.\bar{c}_{L_2,r_2}\langle b\rangle.ALT\langle a, L_1, r_1, b, L_2, r_2\rangle$*, then, for any n, u, v it holds that*

1. $n[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{l,r} \approx n[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{s}}_{l,r'}$.
2. $n[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l,r} \approx n[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{m}}_{l',r'}$.

Proof.

1. We prove that

$$\mathcal{S} \stackrel{\text{def}}{=} \{(n[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{l,r'}, n[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{s}}_{l,r'}) : \forall u, v, l, r, r'\} \bigcup \mathcal{I}$$

is a bisimulation with respect to $\equiv$.
Node n can correctly execute the process ALT only if $r_1, r_2 \leq r_n$. Then the first action to be made is an application of rule (Rad) in order to set the radius to r_1 for transmission of u. Suppose

$$n[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{l,r} \xrightarrow{\tau} n[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{l,r_1}$$

$$n[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{l,r_1} \xrightarrow{c!u@K} \equiv n[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{s}}_{l,r_1}$$

for some set K of locations, then, using (Rad) to set each time the correct radius, (Lose) to discard v and (Obs) to transmit u, we obtain

$$n[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{s}}_{l,r} \stackrel{c!u@K}{\Longrightarrow} \equiv n[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{s}}_{l,r_1}$$

With the same procedure we can show that, if

$$n[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{s}}_{l,r_2} \xrightarrow{c!v@K} \equiv n[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{l,r_2},$$

then:

$$n[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{l,r} \stackrel{c!v@K}{\Longrightarrow} \equiv n[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{l,r_2}.$$

2. We prove that

$$\mathcal{S} \stackrel{\text{def}}{=} \{(n[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l,r}, n[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{m}}_{l',r'}) : \forall l, l', r, r', u, v\} \bigcup \mathcal{I}$$

is a bisimulation up to $\equiv$.
Node n can correctly execute the process ALT only if $r_1, r_2 \leq r_n$. Then the first action to be made is an application of rule (Rad) in order to set the radius to r_1 for transmission of u. Suppose

$$n[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l,r} \xrightarrow{\tau} n[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l,r_1}$$

$$n[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l,r_1} \xrightarrow{c!u@K} \equiv n[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{m}}_{l,r_1}$$

for some set K of locations, then

$$n[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{m}}_{l',r'} \xrightarrow{\tau} n[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{m}}_{l,r'}$$

by applying rule (Move); then, by applying (Rad) to adjust the radius (Lose) to discard v and (Obs) to transmit u, we deduce

$$n[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{m}}_{l',r'} \stackrel{c!u@K}{\Longrightarrow} \equiv n[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{m}}_{l,r_1}.$$

With the same procedure we can prove that, if

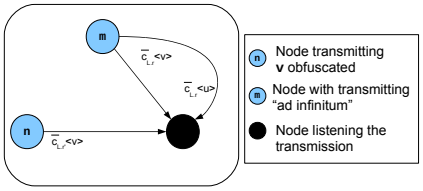
$$n[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{m}}_{l',r_2} \xrightarrow{c!v@K} \equiv n[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l',r_2},$$

then:

$$n[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l,r} \stackrel{c!v@K}{\Longrightarrow} \equiv n[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l',r_2}.$$

Now we have got all the notions to introduce a method to obfuscate messages transmission. A node `m` transmitting "ad infinitum" a messages sequence, may obfuscate the transmission activity of nodes which are transmitting the same messages within the same transmission cell. this happens because nodes that receive a message cannot distinguish the sender, but only the channel of transmission. At a first analysis this property seems to be too much restrictive to be used in concrete situations, but there are many situations where packages transmitted in a network are standard. Consider the example of the network installed for the earthquake area: the ambulances and the hospital can communicate with standard messages. Consider for example the message `v`: "`patient with cardiac arrest`", suppose that `A1` transmits `v` "ad infinitum"

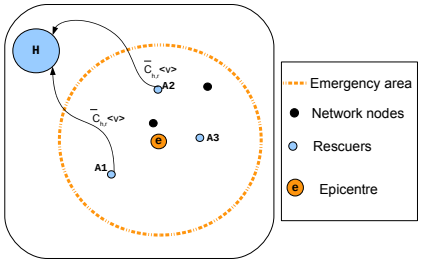
Fig. 6: Obfuscation of the transmission of v from the node n



to be sure that the hospital receives the message correctly. Then also A2 transmits the same package to the server, using the same channel: it could be result that the hospital prepares the acceptance for only one patient, but the patients with cardiac arrest are two. We choose this example to show how a deep analysis of these problems in transmission management are particularly important in mobile ad hoc networks, because this kind of network is used in critical situations.

In our example message obfuscation results to be an obstacle for the good management of networks, a problem rather then a property. In other cases we can prove that the possibility of a node to hide its transmission could be a positive future (as in case of war). A formal model as E-BUM, has the purpose of analysing deeply the characteristics of the networks, with both their positive and negative consequences for the communication management.

Fig. 7: Example of obfuscation in transmission of v by A1



Theorem 6 (Obfuscating message transmission). *Let P and Q be two processes such that $fc(P,Q) \subseteq \{c\}$ for some channel c, where all the output actions of P and Q are in the set $\{\bar{c}_{L_1,r_1}\langle u\rangle, \bar{c}_{L_2,r_2}\langle v\rangle\}$. Then:*

1. $n[P]^{\mathtt{s}}_{k,r}|m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{k,r} \approx n[Q]^{\mathtt{s}}_{k,r}|m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{k,r}$.

2. $n[P]^{\mathtt{m}}_{l_1,r}|m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l_2,r} \approx n[Q]^{\mathtt{m}}_{l_3,r}|m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l_4,r}$.

Proof.

1. As $\approx$ is transitive, We have only to show

$$n[P]^{\mathtt{s}}_{k,r}|m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{k,r} \approx m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{k,r}$$

because we will use the same procedure to prove that

$$n[Q]^{\mathtt{s}}_{k,r}|m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{k,r} \approx m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{k,r}$$

then we can deduce

$$n[P]^{\mathtt{s}}_{k,r}|m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{k,r} \approx m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{k,r} \approx n[Q]^{\mathtt{s}}_{k,r}|m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{k,r}.$$

We then prove the relation

$$\begin{aligned}&\mathcal{S} = \\ &\{(n[P]^{\mathtt{s}}_{k,r}|m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{k,r}, m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{k,r}) : \\ &\qquad \forall u, v, k, r, \\ &\qquad \forall P. fc(P) \subseteq \{c\} \text{ where all output actions of } P \text{ are} \\ &\qquad \{\bar{c}_{L_1,r_1}\langle u\rangle, \bar{c}_{L_2,r_2}\langle v\rangle\}\}\bigcup \mathcal{I}\end{aligned}$$

is a bisimulation up to$\equiv$. We assume for simplicity that both m and n have enough power to set r_1 and r_2 as transmission radius. Suppose then

$$n[P]^{\mathtt{s}}_{k,r}|m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{k,r} \stackrel{c!u@K}{\Longrightarrow} \equiv M$$

for some set K of nodes. if m is the sender of u we have

$$M \equiv n[P]^{\mathtt{s}}_{k,r}|m[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{s}}_{k,r_1}.$$

If n is the sender of message we have

$$M \equiv n[P']^{\mathtt{s}}_{k,r_1}|m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{k,r},$$

where $n[P]^{\mathtt{s}}_{k,r_1} \xrightarrow{c!u@K} n[P']^{\mathtt{s}}_{k,r_1}$. In the first case it simply suffices an application of (Rad) to adjust the radius and (Obs) also to $m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{k,r}$, obtaining $m[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{s}}_{k,r_1}$, whereas in the second case, after an application of (Rad) and (Obs) we use (Lose) to discard v obtaining $m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{k,r_1}$ again. it is easy now to prove that

$$(n[P]^{\mathtt{s}}_{k,r}|m[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{s}}_{k,r_1}, m[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{s}}_{k,r_1})$$

and

$$(n[P']^{\mathtt{s}}_{k,r_1}|m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{k,r}, m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{s}}_{k,r})$$

are members of $\mathcal{S}$, because the same properties of the initial couple are still valid ($fc(P') \subseteq \{c\}$ and all output actions of P' are $\{\bar{c}_{L_1,r_1}\langle u\rangle, \bar{c}_{L_2,r_2}\langle v\rangle\}$), so it suffices the application of the same procedure.

2. As $\approx$ is transitive, it suffices proving

$$n[P]^{\mathtt{m}}_{l_1,r}|m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l_2,r} \approx m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l,r},$$

because we then use the same procedure to demonstrate

$$n[Q]^{\mathtt{m}}_{l_3,r}|m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l_4,r} \approx m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l,r},$$

we then deduce

$n[P]^{\mathtt{m}}_{l_1,r}|m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l_2,r} \approx m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l,r} \approx$
$n[Q]^{\mathtt{m}}_{l_3,r}|m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l_4,r}$.

We now prove that the relation

$\mathcal{S} =$
$\{(n[P]^{\mathtt{m}}_{l_1,r}|m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l_2,r}, m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l,r}) :$
$\forall u, v, l, l_1, l_2, r,$
$\forall P. fc(P) \subseteq \{c\}$ where all output actions of P are
$\{\bar{c}_{L_1,r_1}\langle u\rangle, \bar{c}_{L_2,r_2}\langle v\rangle\}\}\bigcup\mathcal{I}$

is a bisimulation up to $\equiv$. Suppose

$$n[P]^{\mathtt{m}}_{l_1,r}|m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l_2,r} \stackrel{c!u@K}{\Longrightarrow} \equiv M.$$

if m is the sender of u, we have

$$M \equiv n[P]^{\mathtt{m}}_{l_1,r}|m[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{m}}_{l_2,r_1},$$

if n is the sender of the message we have

$$M \equiv n[P']^{\mathtt{m}}_{l_1,r_1}|m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l_2,r},$$

where $n[P]^{\mathtt{m}}_{l_1,r} \stackrel{c!u@K}{\Longrightarrow} n[P']^{\mathtt{m}}_{l_1,r_1}$. In both cases we use the rule (Move), (Rad) and we obtain $m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l,r} \stackrel{\tau}{\Longrightarrow} m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l_2,r_1}$. Then, in the first case it simply suffices an application of rule (Obs) also to $m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l_2,r_1}$ obtaining $m[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{m}}_{l_2,r_1}$, in the second case, after an application of rule (Obs) we use (Lose) to discard v and (Rad) to adjust the radius obtaining $m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l_2,r_1}$ again. it is is easy now to prove that

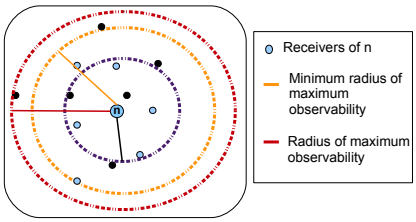
$$(n[P]^{\mathtt{m}}_{l_1,r}|m[ALT\langle v, L_2, r_2, v, L_1, r_1\rangle]^{\mathtt{m}}_{l_2,r_1}, m[ALT\langle v, L_2, r_2, u, L_1, r_1\rangle]^{\mathtt{m}}_{l_2,r_1})$$

and

$$(n[P']^{\mathtt{m}}_{l_1,r_1}|m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l_2,r}, m[ALT\langle u, L_1, r_1, v, L_2, r_2\rangle]^{\mathtt{m}}_{l_2,r_1})$$

are in $\mathcal{S}$ because the same properties of the initial couple are still valid ($fc(P) \subseteq \{c\}$ where all output actions of P are $\{\bar{c}_{L_1,r_1}\langle u\rangle, \bar{c}_{L_2,r_2}\langle v\rangle\}$), so it suffices applying the same procedure.

Fig. 8: Radii of maximum observability



5.4 Radius of maximum observability

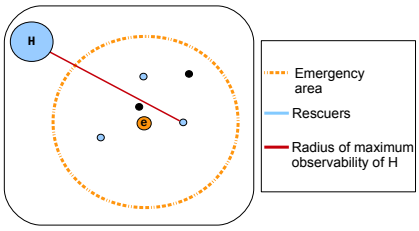
All the properties described above can be proved also in the original CMN [14]; now we introduce new properties which cannot be dealt with in CMN.

The first important characteristic we are going to describe is about the transmission radius of the nodes. Each transmission is associated to a set of locations including the receivers of the message. Then we can define a "*radius of maximum observability*", that is a radius such to allow a correct reception of a message to all the locations of the receivers set. In particular we can define the "*minimum radius of maximum observability*", which corresponds to the distance between the sender of the message and the most distant receiver. Figure 8 illustrates three different cases of a transmission effect in a network: the black radius (the smallest) does not allow the reception of the message by the set of the receivers (light nodes) while the other two radii reach at least one of the receivers. The orange radius is in particular the distance between the transmitter and the most distant receiver: This characteristic means that this is the *minimum radius of maximum observability*.

To understand how this property is important let consider the example depicted in Figure 9. The earthquake has damaged a defined area; we can than deduce that rescuers need to communicate only within the emergency area (in figure the area delimited by the orange circle). We can then determine the minimum transmission radius which ensures the central server of the hospital to be able to communicate with the ambulances sent for assistance in the disaster area. This property is important only for stationary nodes, whereas a mobile node can move within the transmission cell of the transmitter to receive the communication. In our example the central server needs to communicate with the ambulances, which are all mobile nodes, then instead of determining the minimum radius of maximum observability, which change arbitrarily, it is better considering a radius enough large to ensure the correct result of the transmission within all the emergency area.

Although we can define a minimum radius to reach all the intended receivers of a transmission, we cannot be sure of the correct reception of the message

Fig. 9: determination of the minimum radius of maximum observability



by the whole set of intended receivers; There are indeed various obstacles (as connection failures, ore physical barriers to transmissions...) which can obstruct the correct outcome of a transmission in the network; This is the reason why the output actions are always observable, while the input actions are not.

Theorem 7 (Radius of maximum observability). *Let $n[P]^{\mathtt{s}}_{l,r}$ be a stationary node located at l such that $\mathtt{rcv}(P) = L$, and $d(l,k) \leq r_n$ for all $k \in L$. Then:*

$$n[P]^{\mathtt{s}}_{l,r} \approx m[P]^{\mathtt{s}}_{l,r'} \text{ for every node } m \text{ such that } r_m \geq r_n$$

In this case we say that r_n is a radius of maximum observability for the stationary process $n[P]^{\mathtt{s}}_{l,r}$.

Proof. 0 We prove that the relation

$$\mathcal{S} = \{(n[P]^{\mathtt{s}}_{l,r}, m[P]^{\mathtt{s}}_{l,r'}) : \\ \forall r_m \geq r_n,\ \forall l, \\ \forall P.\mathtt{rcv}(P) = L\} \bigcup \mathcal{I}$$

is a bisimulation.
Consider

$$n[P]^{\mathtt{s}}_{l,r} \xrightarrow{c!v@L_i} n[P']^{\mathtt{s}}_{l,r}, \text{ with } L_i \subseteq L.$$

Then, by applying rule (Obs) backward it must be $n[P]^{\mathtt{s}}_{l,r} \xrightarrow{c_{L_i}!v[l,r]} n[P']^{\mathtt{s}}_{l,r}$, as $d(l,l_i) \leq r \forall l_i \in L_i \subseteq L$, and by applying rule (Snd) backward we finally obtain $P \xrightarrow{\bar{c}_{L_i,r}v} P'$. So, by applying rule (Rad), as $r \leq r_n \leq r_m$ we can write

$$m[P]^{\mathtt{s}}_{l,r'} \xrightarrow{\tau} m[P']^{\mathtt{s}}_{l,r}$$

and we can immediately deduce

$$m[P]^{\mathtt{s}}_{l,r} \xrightarrow{c!v@L_i} m[P']^{\mathtt{s}}_{l,r}$$

Now it is sufficient to prove that

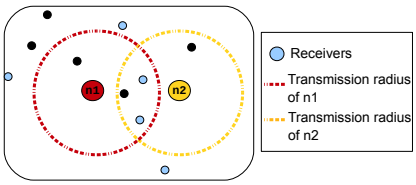
$$n[P']^{\mathtt{s}}_{l,r} \mathcal{S}m[P']^{\mathtt{s}}_{l,r}$$

We know that for P' the same properties of P are valid ($\mathtt{rcv}(P') \subseteq L$ for definition of the function $\mathtt{rcv}(\cdot)$), we can then apply to P' the same procedure used for P.

Definition 7 (Minimum Radius of Maximum observability). *Let $n[P]^{\mathtt{s}}_{l,r}$ be a stationary node located at l such that $\mathtt{rcv}(\mathtt{P}) = L$ and r_n is a radius of maximum observability for $n[P]^{\mathtt{s}}_{l,r}$. A radius r' is said to be the minimum radius of maximum observability for $n[P]^{\mathtt{s}}_{l,r}$ if $r' \leq r_n$ and for all $k \in L$ it holds that $d(l,k) \leq r'$ and for all $r'' \leq r'$ there exists $k' \in L$ such that $d(l,k') > r''$.*

5.5 Simulation of stationary nodes in different locations

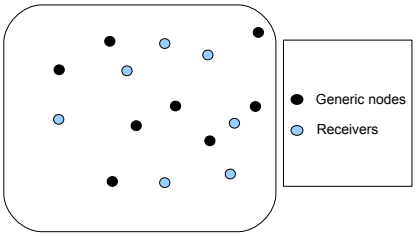
Fig. 10: Example of simulation of stationary nodes in different locations



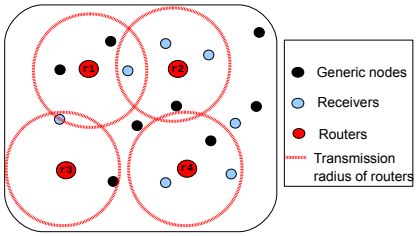
The tag L associated to each output action has been introduced, not only in order to find the minimum radius ensuring each transmission to reach all its receivers, but its introduction allows us to define other important properties for our calculus. If we pay attention to the behaviour of stationary nodes, we realise that the tag L enables, under particular prerequisites, the simulation of stationary devices in different locations. In our calculus the barb of a transmission is not determined by a set of locations, but by the intersection of two sets: more precisely the barb of a transmission is given by the set of locations which are members of L, lying in the transmission cell of the sender. By these assumptions, we can now consider the case where two stationary nodes, placed in different locations (with therefore different neighbours), but communicating with the same set of locations, result to have the same barb. A practical example of the usefulness of this property is the case we have to use the lowest number of routers within an area in order to ensure the communication with a given set of locations. If we realise that two different routers result to have the same behaviour, one of them can be then turn off, allowing us to save power and physical resources. Looking at Figure 11 we can see an example of optimising

Fig. 11: Example of optimising routers allocation

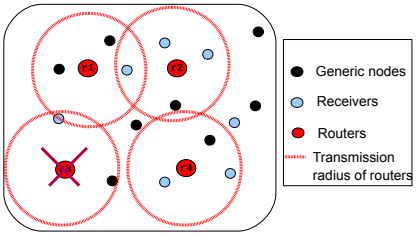
(a) initial network topology



(b) First routers allocation



(c) Optimal routers allocation



the allocation of the routers, by turning off the router `r3`, which is not usefull, because it can be simulated by `r1`.

Theorem 8 (Simulation of stationary nodes in different locations). *Let $n[P]^{\mathtt{s}}_{l_n,r_n}$ and $m[P]^{\mathtt{s}}_{l_m,r_m}$ be two stationary nodes located at l_n and l_m respectively. Assume $\mathtt{rcv}(P) = L$, $r \leq r_n \wedge r \leq r_m$ for all r associated with P output actions. Finally assume $K = \{k \mid d(l_n, k) \leq r_n \wedge k \in L\}$ and $K' = \{k \mid d(l_m, k) \leq r_m \wedge k \in L\}$. it holds that:*

1. *If $K' \subseteq K$, then $n[P]^{\mathtt{s}}_{l_n,r_n}$ simulates $m[P]^{\mathtt{s}}_{l_m,r_m}$;*
2. *If $K = K'$, then $n[P]^{\mathtt{s}}_{l_n,r_n} \approx m[P]^{\mathtt{s}}_{l_m,r_m}$.*

Proof.

1. the interesting case to analyse is the output action. Consider $P = \bar{c}_{L_i,r}\langle v\rangle.P'$ for some $L_i \subseteq L$. Then using (Rad):

   $$m[P]^{\mathtt{s}}_{l_m,r_m} \xrightarrow{\tau} m[P]^{\mathtt{s}}_{l_m,r}.$$

   Then by an application of (Obs)

   $$m[P]^{\mathtt{s}}_{l_m,r} \xrightarrow{c!v@K''} m[P']^{\mathtt{s}}_{l_m,r}, \text{ where } K'' = K' \cap L_i$$

   Then we can write

   $$n[P]^{\mathtt{s}}_{l,r_n} \overset{c!v@K'''}{\Longrightarrow} n[P']^{\mathtt{s}}_{l_n,r} \text{ where } K''' = K \cap L_i.$$

   But, as $K' \subseteq K$, we deduce $K' \cap L_i = K'' \subseteq K''' = K \cap L_i$ and, by applying rule (Lose) to discard all elements of K''' that are not elements of K'', we can also write

   $$n[P]^{\mathtt{s}}_{l_n,r_n} \overset{c!v@K''}{\Longrightarrow} n[P']^{\mathtt{s}}_{l_n,r}.$$

   As $\mathtt{rcv}(P') \subseteq L$, by applying the same procedures to P' we can prove that $n[P']^{\mathtt{s}}_{l_n,r}$ simulates $m[P']^{\mathtt{s}}_{l_m,r}$.
2. If $K = K'$ then $K \subseteq K'$ and $K' \subseteq K$; so, by applying the same procedure used to prove the first item of this theorem, we demonstrate that the relation

   $$\mathcal{S} = \{(n[P]^{\mathtt{s}}_{l_n,r_n}, m[P]^{\mathtt{s}}_{l_m,r_m}) : \forall P.\mathtt{rcv}(P) \subseteq L\} \bigcup \mathcal{I}$$

   is a bisimulation.

5.6 Range repeaters

We are going to define the *Range Repeaters*, that are devices which regenerate a network signal in order to extend the range of the existing network infrastructure. A definition of repeater was already given in [14]. Here we give a new definition of range repeater for E-BUM, and we use both range repeaters with one and two channels to prove new important properties.

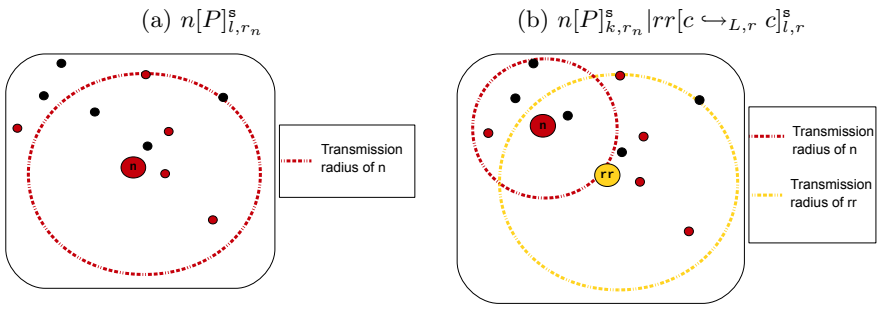
Definition 8. *Let a, b be channels, l a location, r a transmission radius and L a set of locations. A repeater with two channels on L is a stationary device, denoted $rr[a \hookrightarrow_{L,r} b]^{\mathtt{s}}_{l,r_{rr}}$, where $a \hookrightarrow_{L,r} b$ is a process whose general recursive definition is:*

$$a \hookrightarrow_{L,r} b \stackrel{\text{def}}{=} a(x).\bar{b}_{L,r}\langle x\rangle.a \hookrightarrow_{L} b.$$

A range repeater with two channels receive values through the input channel and retransmits them through the output channels, to the message receivers. A range repeater with one channel operates analogously, but input and output channels coincide.

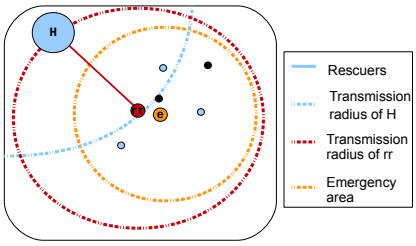
Definition 9. *Let c be a channel, l a location, r a transmission radius and L a set of locations. A range repeater with one channel on L is a stationary device, denoted $rr[c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r_{rr}}$.*

Fig. 12: Range repeater with one channel



Range repeaters are usually exploited to enlarge transmission cell of a stationary node and, if such a node always communicates with the same set of devices, each time through the same channel, by using a range repeater we can simulate the presence of the sender in the location of the repeater. The employment of range repeaters is particularly interesting for Ad-Hoc Networks, because it allows us to analyse and try to solve the problems of a device's mobility. Consider once again the example used in this section. Describing the situation we did not consider the distance between the hospital and the earthquake area, which may be too large to guarantee the communication with the ambulances running up in the emergency area. It will be then necessary employing a range repeater enough powerful to cover all the area and, at the same time, reachable by the central server of the hospital. If the earthquake epicenter is too distance from the hospital we can install a series of consecutive repeaters, which will connect the central server to the disaster area.

Fig. 13: Example of repeaters use



Theorem 9 (Range repeaters with one channel). *Let $n[P]^{\mathtt{s}}_{l,r_n}$ a node executing a process P such that $fc(P) \subseteq \{c\}$ for some channel c, and r is fixed for all the transmissions in P. Let $\mathtt{rcv}(P) = L$. Let $rr[c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r_{rr}}$ a range repeater, k, l be physical locations, $r \leq r_n$, $r \leq r_{rr}$ and $d(k,l) \leq r$. Then:*

$$n[P]^{\mathtt{s}}_{k,r_n} | rr[c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r_{rr}} \text{ simulates } n[P]^{\mathtt{s}}_{l,r_n}.$$

Proof. We have to prove that the relation

$$\begin{array}{c}\mathcal{S} \stackrel{\text{def}}{=} \{(n[P]^{\mathtt{s}}_{l,r_n}, n[P]^{\mathtt{s}}_{k,r_n} | rr[c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r_{rr}}) : \\ \forall l,k,r.d(k,l) \leq r \\ \forall P.fc(P) \subseteq \{c\} \ \wedge \ \mathtt{rcv}(P) = L \ \wedge \ r \leq r_{rr} \ \wedge \ r \leq r_n\}\end{array}$$

is a simulation.
The first rule to be applied, in order to adjust the radius according to the protocol used is (Rad):

$$n[P]^{\mathtt{s}}_{l,r_n} \xrightarrow{\tau} n[P]^{\mathtt{s}}_{l,r}$$

Now suppose:

$$n[P]^{\mathtt{s}}_{l,r} \xrightarrow{c!v@K} n[P']^{\mathtt{s}}_{l,r}$$

for $K = \{k_1, ..., k_n : k_i \in L_i \wedge d(l,k_i) \leq r \ \forall 1 \leq i \leq n\}$, because $P \xrightarrow{\bar{c}_{L_i,r}v} P'$ for some $L_i \subseteq L$. By applying rule (Rad) we adjust the radius of node n, and we can apply (Bcast) to obtain:

$$n[P]^{\mathtt{s}}_{k,r} | rr[c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r_{rr}} \xrightarrow{c_{L_i}!v[k,r]} n[P']^{\mathtt{s}}_{k,r} | rr[\bar{c}_{L,r}\langle v\rangle.c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r_{rr}},$$

and, by applying (Rad) also to the repeater and then rule (Obs),

$$\begin{array}{c}n[P']^{\mathtt{s}}_{k,r} | rr[\bar{c}_{L,r}\langle v\rangle.c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r} \xrightarrow{c!v@K'} n[P']^{\mathtt{s}}_{k,r} | rr[c \hookrightarrow_{L} c]^{\mathtt{s}}_{l,r}, \text{ where} \\ K' = \{k'_1, ..., k'_n : k'_i \in L \wedge d(l,k'_i) \leq r \ \forall 1 \leq i \leq n\}\end{array}$$

that means:

$$n[P]^{\mathtt{s}}_{k,r'} | rr[c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r} \stackrel{c!v@K'}{\Longrightarrow} n[P']^{\mathtt{s}}_{k,r} | rr[c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r}$$

But, as $L_i \subseteq L$ then $K \subseteq K'$, by using rule (Lose) to hide the communications with nodes at locations in K' which are not in K we can finally write:

$$n[P]^{\mathtt{s}}_{k,r} | rr[c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r} \stackrel{c!v@K}{\Longrightarrow} n[P']^{\mathtt{s}}_{k,r} | rr[c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r}$$

We have now only to prove that

$$(n[P']^{\mathtt{s}}_{l,r}, n[P']^{\mathtt{s}}_{k,r} | rr[c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r}) \in \mathcal{S}$$

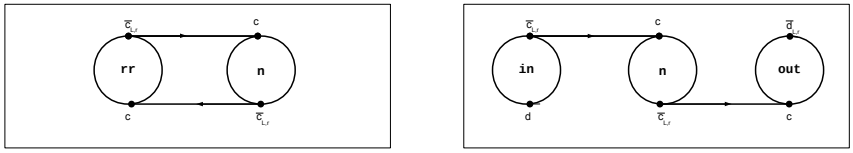
Since for P' the same properties of P are still valid ($fc(P') \subseteq \{c\} \wedge \mathtt{rcv}(P') \subseteq L$) we can apply the same procedure and prove in this way the simulation.

The simulation just described can be realised also with a range repeater with two channels. Using two channels however we need two range repeaters, respectively for input ($\mathtt{in}[d \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r_{\mathtt{in}}}$) and output ($\mathtt{out}[c \hookrightarrow_{L,r} d]^{\mathtt{s}}_{l,r_{\mathtt{out}}}$) management. The diagram in figure 14 illustrates the employment of the channels and the interaction between the nodes in the realisation of range repeaters with one or two channels. This figure is inspired to the diagrams of Milner [16] in his introduction to CCS, describing the behaviour of agents and the use of channels for data input and output. We emphasise that this kind of diagrams gives no information about physical position of nodes or about network topology, but it only shows the connections through which devices can exchange data.

Fig. 14: Range repeaters: diagram of the interaction between the nodes

(a) $rr[c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r_{rr}}$

(b) $\mathtt{in}[d \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r} | n[P]^{\mathtt{s}}_{k,r_n} | \mathtt{out}[c \hookrightarrow_{L,r} d]^{\mathtt{s}}_{l,r}$



Theorem 10 (Range repeaters with two channels). *Let $n[P]^{\mathtt{s}}_{l,r_n}$ be a node executing a process P such that $fc(P) \subseteq \{c\}$, $\mathtt{rcv}(P) = L$ and r is a fixed radius for all the transmissions in P ($r \leq r_n$). Let k be physical location such that $d(k,l) \leq r$. Then, for any channel d:*
$n[P]^{\mathtt{s}}_{k,r_n} | \mathtt{out}[c \hookrightarrow_{L,r} d]^{\mathtt{s}}_{l,r} | \mathtt{in}[d \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r}$ simulates $n[\{d/c\}P]^{\mathtt{s}}_{l,r_n}$ (with $r \leq r_{\mathtt{in}} \wedge r \leq r_{\mathtt{out}}$).

Proof. Proof is given with the same method used for the previous theorem, so we prove that the relation

$$\mathcal{S} \stackrel{\text{def}}{=} \{(n[\{d/c\}P]^{\mathtt{s}}_{l,r_n}, n[P]^{\mathtt{s}}_{k,r_n}|\mathtt{out}[c \hookrightarrow_{L,r} d]^{\mathtt{s}}_{l,r}|\mathtt{in}[d \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r}) : \forall l,k,r.d(k,l) \leq r \ \wedge \ d(l,k) \leq r \quad \forall P.fc(P) \subseteq \{c\} \ \wedge \ \mathtt{rcv}(P) = L \quad r \leq r_n \wedge r \leq r_{\mathtt{in}} \wedge r \leq r_{\mathtt{out}}\}$$

is a simulation. Suppose that node $n[P]^{\mathtt{s}}_{l,r_n}$, by applying Rule (Rad) adjusts its transmission radius and than execute an output action:

$$n[\{d/c\}P]^{\mathtt{s}}_{l,r} \xrightarrow{d!v@K} n[\{d/c\}P']^{\mathtt{s}}_{l,r}$$

for $K = \{k_1, ..., k_n : k_i \in L_i \wedge d(l,k_i) \leq r \, \forall \, 1 \leq i \leq n\}$ because $P \xrightarrow{\bar{c}_{L_i,r}v} P'$ for some $L_i \subseteq L$. knowing that $d(k,l) \leq r$, by applying rule (Rad) and (Bcast) we obtain

$$n[P]^{\mathtt{s}}_{k,r_n}|\mathtt{out}[c \hookrightarrow_{L,r} d]^{\mathtt{s}}_{l,r}|\mathtt{in}[d \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r} \xrightarrow{c_{L_i}!v[k,r]} n[P']^{\mathtt{s}}_{k,r}|\mathtt{out}[\bar{d}_{L,r}\langle v\rangle.c \hookrightarrow_{L,r} d]^{\mathtt{s}}_{l,r}|\mathtt{in}[d \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r}.$$

Now we can exploit the repeater $\mathtt{out}$, created on purpose for output actions. By applying first rule (Bcast) and later rule (Obs) we obtain:

$$n[P']^{\mathtt{s}}_{k,r}|\mathtt{out}[\bar{d}_{L,r}\langle v\rangle.c \hookrightarrow_{L} d]^{\mathtt{s}}_{l,r}|\mathtt{in}[d \hookrightarrow_{L} c]^{\mathtt{s}}_{l,r} \stackrel{d!v@K'}{\Longrightarrow} n[P']^{\mathtt{s}}_{k,r'}|\mathtt{out}[c \hookrightarrow_{L} d]^{\mathtt{s}}_{l,r}|\mathtt{in}[d \hookrightarrow_{L} c]^{\mathtt{s}}_{l,r}$$

with $K' = \{k'_1, ..., k'_m : k'_i \in L \wedge d(l,k'_i) \leq r \, \forall \, 1 \leq i \leq m\}$. Then:

$$n[P]^{\mathtt{s}}_{k,r}|\mathtt{out}[c \hookrightarrow_{L,r} d]^{\mathtt{s}}_{l,r}|\mathtt{in}[d \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r} \stackrel{d!v@K'}{\Longrightarrow} n[P']^{\mathtt{s}}_{k,r}|\mathtt{out}[c \hookrightarrow_{L,r} d]^{\mathtt{s}}_{l,r}|\mathtt{in}[d \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r}.$$

As $L_i \subseteq L$ we deduce that also $K \subseteq K'$ and, by applying rule (Lose) to discard all the locations in K' which are not in K we can also write:

$$n[P]^{\mathtt{s}}_{k,r}|\mathtt{out}[c \hookrightarrow_{L,r} d]^{\mathtt{s}}_{l,r}|\mathtt{in}[d \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r} \stackrel{d!v@K}{\Longrightarrow} n[P']^{\mathtt{s}}_{k,r}|\mathtt{out}[c \hookrightarrow_{L,r} d]^{\mathtt{s}}_{l,r}|\mathtt{in}[d \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r}$$

Now it is sufficient to prove that

$$(n[\{d/c\}P']^{\mathtt{s}}_{l,r}, n[P']^{\mathtt{s}}_{k,r}|\mathtt{out}[c \hookrightarrow_{L,r} d]^{\mathtt{s}}_{l,r}|\mathtt{in}[d \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r}) \in \mathcal{S}$$

Since for P' the same properties of P are still valid ($fc(P') \subseteq \{c\} \wedge \mathtt{rcv}(P') \subseteq L$), by applying the same procedure used for P we can prove the simulation.
Suppose now that an input action is executed, then we use $\mathtt{in}$. Suppose:

$$n[\{d/c\}P]^{\mathtt{s}}_{l,r_n} \xrightarrow{d?v@l} n[\{d/c\}\{v/x\}P']^{\mathtt{s}}_{l,r_n}$$

because $P \xrightarrow{cv} \{v/x\}P'$. Since it lies in location l, also $\mathtt{in}$ can receive v through channel d. In particular we have:

$$n[P]^{\mathtt{s}}_{k,r_n}|\mathtt{out}[c \hookrightarrow_{L,r} d]^{\mathtt{s}}_{l,r}|\mathtt{in}[d \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r} \xrightarrow{d?v@l} n[P]^{\mathtt{s}}_{k,r_n}|\mathtt{out}[c \hookrightarrow_{L,r} d]^{\mathtt{s}}_{l,r}|\mathtt{in}[\bar{c}_{L,r}\langle v\rangle.d \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r}$$

Now, by applying rule (Bcast), recalling that $P = c(x).P'$, we can write:

$$n[P]^{\mathtt{s}}_{k,r_n}|\mathtt{out}[c \hookrightarrow_{L,r} d]^{\mathtt{s}}_{l,r}|\mathtt{in}[\bar{c}_{L,r}\langle v\rangle.d \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r} \xrightarrow{c_L!v[l,r]} n[\{v/x\}P']^{\mathtt{s}}_{k,r}|\mathtt{out}[c \hookrightarrow_{L,r} d]^{\mathtt{s}}_{l,r}|\mathtt{in}[d \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r}$$

We can then deduce:

$$n[P]^{\mathtt{s}}_{k,r_n}|\mathtt{out}[c \hookrightarrow_{L,r} d]^{\mathtt{s}}_{l,r}|\mathtt{in}[d \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r} \stackrel{d?v@l}{\Longrightarrow} n[\{v/x\}P']^{\mathtt{s}}_{k,r_n}|\mathtt{out}[c \hookrightarrow_{L,r} d]^{\mathtt{s}}_{l,r}|\mathtt{in}[d \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r}$$

Now it is sufficient to prove that

$$(n[\{d/c\}\{v/x\}P']^{\mathtt{s}}_{l,r_n}, n[\{v/x\}P']^{\mathtt{s}}_{k,r_n}|\mathtt{out}[c \hookrightarrow_{L,r} d]^{\mathtt{s}}_{l,r}|\mathtt{in}[d \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r}) \in \mathcal{S}$$

Since for P' the same properties of P are still valid ($fc(P') \subseteq \{c\} \wedge \mathtt{rcv}(P') \subseteq L$), by applying the same procedure we can finally prove the simulation.

Defining the *Minimum Radius of Maximum Observability*, we have emphasised the importance of ensuring that a message transmission can reach the whole set of intended receivers. By applying this concept to the definition of range repeater, we can introduce the notion of *complete range repeater*, that is a repeater which has a radius enough large to reach all the locations in the set of receivers.

Definition 10 (Complete range repeater). *We define the repeater complete on L as a repeater $rc[c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r_{rc}}$ (with $r \leq r_{rc}$) whose barb coincides with L, i.e., $rc[c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r_{rc}} \Downarrow_c$ and $d(l,k) \leqslant r \forall k \in L$.*

Looking at the example in Figure 13, where we suppose that a repeater is installed to allow the central server of the hospital to communicate with the ambulances, we can notice how the repeater has been chosen such to guarantee that its transmission radius (the red segment in figure) covers the complete area of the disaster (orange line in figure). This is also an example of a complete range repeater, whose radius is a radius of maximum observability for the entire earthquake area. The use of a complete range repeater reduces the problem of ensuring the communication between the central server and a set of locations, to the communication between only two devices: H will be then sure that, in whatever locations the ambulances will lie, they will be always reachable by rr.

Theorem 11 (Complete range repeaters). *Let $n[P]^{\mathtt{s}}_{k,r_n}$ be a stationary node, with P such that $\mathtt{rcv}(P) = L$, $fc(P) \subseteq \{c\}$ and r_{min} the minimum radius associated to the output actions of P. Let $rc[c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r_{rc}}$ be a complete range repeater on L, lying at location l, with radius r . Then:*
$n[P]^{\mathtt{s}}_{k,r_n}|rc[c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r_{rc}} \Downarrow_c \forall k.d(k,l) \leq r_{min}$, and all the recipients of L will be reachable by the node n. It means that, for each fragment of the process P executing an output action $\bar{c}_{L_i,r_i}\langle v_i\rangle.Q$ such that $P = P'.\bar{c}_{L_i,r_i}\langle v_i\rangle.Q$ it holds $n[\bar{c}_{L_i,r_i}\langle v_i\rangle.Q]^{\mathtt{s}}_{k,r_n}|rc[c \hookrightarrow_L c]^{\mathtt{s}}_{l,r_n} \stackrel{c!v@L_i}{\Longrightarrow} n[Q]^{\mathtt{s}}_{k,r_n}|rc[c \hookrightarrow_L c]^{\mathtt{s}}_{l,r_{rc}}$

Proof. Let consider $P = P_1.\bar{c}_{L_1,r_1}\langle v_1\rangle.Q$, and $\bar{c}_{L_1,r_1}\langle v_1\rangle$ is the first output action in process P (we can write $P \stackrel{\tau}{\Longrightarrow} \bar{c}_{L_1,r_1}\langle v_1\rangle.Q$). We can write

$$n[P]^{\mathtt{s}}_{k,r_n} \overset{c_{L_1,r_1}!v_1[k,r_1]}{\Longrightarrow} n[Q]^{\mathtt{s}}_{j,r_1}$$

since $d(l,k) \leq r_1$ we have

$$n[P]^{\mathtt{s}}_{k,r_n}|rc[c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r_{rc}} \overset{c_{L_1}!v_1[k,r_1]}{\Longrightarrow} n[P']^{\mathtt{s}}_{k,r_1}|rc[\bar{c}_{L,r}\langle v\rangle.c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r_{rc}}$$

By applying rule (Rad) to adjust the radius and then (Bcast) we can write

$$\mathtt{l}\; n[P']^{\mathtt{s}}_{k,r_1}|rc[\bar{c}_{L,r}\langle v\rangle.c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r_{rc}} \overset{c_L!v_1[l,r]}{\Longrightarrow} n[P']^{\mathtt{s}}_{k,r_1}|rc[c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r}$$

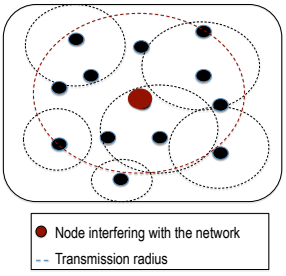
By applying rule (Obs), knowing that $L_1 \subseteq L$ and consequently $d(l,k) \leq r\; \forall k \in L_1$ we can use (Lose) to discard all the elements of L which are not in L_1 and write

$$n[P]^{\mathtt{s}}_{k,r_1}|rc[c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r_{rc}} \overset{c!v_1@L_1}{\Longrightarrow} n[P']^{\mathtt{s}}_{k,r_1}|rc[c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r}$$

By our definition of Barb, using Harmony theorem we can deduce also $n[P]^{\mathtt{s}}_{k,r_n}|rc[c \hookrightarrow_{L,r} c]^{\mathtt{s}}_{l,r_{rc}} \Downarrow_c$ and the set of receivers is L because $d(k,l) \leq r\; \forall k \in L$. For the successive output actions of the process P the proof is similar because we know that each $L_i \subseteq L$ is completely reachable by the range repeater used.

6 Reducing interference in order to avoid unnecessary power consumption

Fig. 15: Example of Interference: a node with a too large transmission energy may disturb the other transmission within the network



As mentioned above, reducing interference is one of the main goals of topology control besides direct energy conservation by restriction of transmission power. For example, looking at Figure 15 we can observe that the red node has got a transmission radius large enough to reach all the nodes of the network: this is not a positive characteristic because it means a large energy consumption, together

with a higher interference with other transmissions and a consequent network congestion.

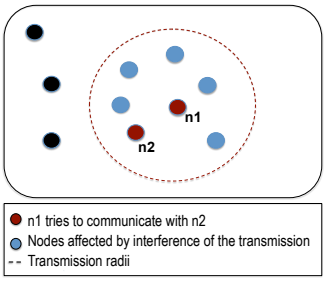
Most of the proposed topology control algorithms try to reduce interference implicitly as a consequence of sparseness or low degree of the resulting topology graph. An explicit concept of interference, based on the current network traffic, has been proposed in [15], while an explicit definition that is independent on the network traffic has been presented in [4]. This definition is based on the question how many nodes are affected by communication over a given link. In contrast the definition presented in [9] considers interference at the intended receiver of a message.

Following we will try to give a definition of *Interference* for Mobile Ad Hoc Networks. We will consider two different approaches to the problem:

1. The first approach will consist in a *Sender-centered* definition of Interference considering the amount of noise caused by a certain transmission
2. The second approach will define instead a *Receiver-centered* Interference, which considers the amount of noise caused on a given transmission

6.1 Sender-centered Interference

Fig. 16: Example of interference caused by a transmission



Following the definition introduced in [4], the notion of *Sender-centered Interference* arises from a natural question: How many nodes are disturbed by a given communication over the network?

Consider the situation depicted in Figure 16 where a node $n1$ is intended to transmit a message to $n2$. We can define Sender-centered Interference as the number of nodes listening to the message, but not interested in receiving it.

Definition 11 (Level of Sender-centered Interference). *Let* $c_L!\tilde{v}[l,r]$ *be an output action,* H *be the set of possible locations of the nodes in the network and* $K = \{k \in H : \ d(l,k) \leq r\}$. *The* level of Sender-centered Interference *relative to this output is defined as:*

$$I_{send}(c_L!\tilde{v}[l,r]) = |K - L|.$$

Once we have explained the notion of interference, given a transmission, if the set of nodes not interested in receiving the transmission is empty, we can affirm that there is no interference in the communication , i.e. if $I_{send}(c_L!\tilde{v}[l,r]) = 0$.

The E-BUM calculus allows us to observe the case in which a transmission reaches only its intended receivers, without any interference. Indeed, we can compare the behaviour of a node communicating with a given set L of recipients, with the behaviour of the same node but broadcasting all its communications to the whole network. If the two behaviours are related by $\cong$, then we can affirm that the node transmissions do not provoke any interference, in other words they do not disturb any other node in the network.

Let us first define the broadcasting version of a process P, denoted by $brd(P)$, as follows:

- if $P = \mathbf{0}$ then $brd(P) = \mathbf{0}$;
- if $P = c(\tilde{x}).P'$ then $brd(P) = c(\tilde{x}).brd(P')$;
- if $P = \bar{c}_{L,r}\langle\tilde{v}\rangle.P'$ then $brd(P) = \bar{c}_{\infty,r}\langle\tilde{v}\rangle.brd(P')$.
- if $P = [w_1 = w_2]Q, R$ then $brd(P) = [w_1 = w_2]brd(Q), brd(R)$.

Definition 12 (Absence of Sender-centered Interference). *We say that a node $n[P]^{\mu}_{l,r}$ is free of* Sender-centered interference *if*

$$n[P]^{\mu}_{l,r} \cong n[brd(P)]^{\mu}_{l,r}.$$

Notice that, by contextuality, if $n[P]^{\mu}_{l,r} \cong n[brd(P)]^{\mu}_{l,r}$ then also $n[P]^{\mu}_{l,r} \mid M \cong n[brd(P)]^{\mu}_{l,r} \mid M$ for any network M. This means that if $n[P]^{\mu}_{l,r}$ is free of *Sender-centered interference*, independently of the behaviour of the other nodes in the network.

Theorem 12 (Absence of Sender-centered Interference). *If $n[P]^{\mu}_{l,r}$ is free of* Sender-centered Interference *then for all output actions $c_L!\tilde{v}[l,r]$ performed by $n[P]^{\mu}_{l,r}$ it holds that $I_{send}(c_L!\tilde{v}[l,r]) = \emptyset$.*

Proof. We will give a proof by contradiction. Since $n[P]^{\mu}_{l,r}$ is free of *Sender-centered Interference* we can write:

$$n[P]^{\mu}_{l,r} \cong n[brd(P)]^{\mu}_{l,r}$$

Let consider a derivative $n[P']^{\mu}_{l',r}$ of $n[P]^{\mu}_{l,r}$ such that $n[P']^{\mu}_{l',r} \xrightarrow{c_L!v[l',r]} n[P'']^{\mu}_{l',r}$. Since $n[P]^{\mu}_{l,r} \cong n[brd(P)]^{\mu}_{l,r}$ there exists a derivative $n[Q']^{\mu}_{l'',r}$ of $n[brd(P)]^{\mu}_{l,r}$ such that $n[P']^{\mu}_{l',r} \cong n[Q']^{\mu}_{l'',r}$. Now suppose by contradiction that $I_{send}(c_L!v[l',r]) > 0$. Then, by definition of Interference it holds that there exists k such that $d(l',k) \leq r$ and $k \notin L$. If we apply rule (Obs) to $n[Q']^{\mu}_{l'',r}$, assuming that only k could receive $\tilde{v}$, then we will write:

$$n[Q']^{\mu}_{l'',r} \xrightarrow{c!\tilde{v}@k} n[Q'']^{\mu}_{l'',r}$$

But we cannot write:

$$n[P']^{\mu}_{l',r} \stackrel{c!\tilde{v}@k}{\Longrightarrow} n[P'']^{\mu}_{l',r}$$

because $k \notin L$. Since we assumed that $n[P']^{\mu}_{l',r} \cong n[Q']^{\mu}_{l'',r}$, we reached a contradiction.

We may be interested in verifying the absence of Sender-centered Interference relative to a specific set of nodes S. This can be done by defining the broadcasting version of a process P relative to S, noted $brd(S,P)$. The definition of $brd(S,P)$ analogous to the one of $brd(P)$ except for the third item that is

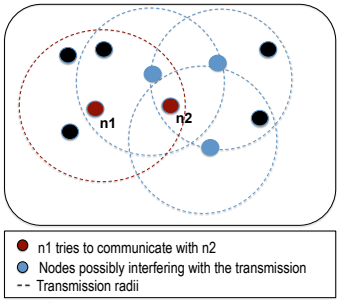
– if $P = \bar{c}_{L,r}\langle\tilde{v}\rangle.P'$ then
$brd(P,S) = \bar{c}_{L\cup S,r}\langle\tilde{v}\rangle.brd(P',S)$

In this case, we obtain that a node $n[P]^{\mu}_{l,r}$ is free of *Sender-centered Interference* relative to S if

$$n[P]^{\mu}_{l,r} \cong n[brd(P,S)]^{\mu}_{l,r}.$$

6.2 Receiver-centered Interference

Fig. 17: Example of interference suffered by a transmission



The second approach we adopt in order to give a good definition of Interference will focus the attention to the behaviour of the whole network around a node which is taking part to a certain transmission (see [27, 9]). Let us consider the example depicted in Figure 17: $n1$ is trying to transmit a message to $n2$, but $n2$ lies in the transmission cell of three other devices of the network, which, with their transmissions, could prevent $n2$ to receive the message sent by $n1$.

Since in the previous section we paid our attention to specific output actions, in order to measure how much noise may they provoke to the networks, in this case our goal will be the analysis of the conditions of single locations, with respect to the environment surrounding them.

Following we introduce the level of Receiver-centered Interference as an upper bound of the quantity of noise possibly provoked by a network M to a location l.

Definition 13 (Level of Receiver-centered Interference). *Let M be a network consisting of k devices:*

$$M = n_1[P_1]^{\mu_1}_{l_1,r_1} \mid ... \mid n_k[P_k]^{\mu_k}_{l_k,r_k},$$

then the level of Receiver-centered Interference *with respect to a given location l is defined as:*

$$I_{rec}(l, M) = |\{j \in \{1, \ldots, k\}.\ d(l, l_j) \leq r_j \wedge \\ l \notin dest(P_j) \wedge dest(P_j) \neq 0\}|$$

where r_j is the maximum transmission radius which the process P_j set for n_j's communications. The last condition, $dest(P_j) \neq 0$, ensures that only those nodes which are active, i.e., execute at least one output action, are considered.

As we have done above, we use the E-BUM calculus to provide an efficient proof technique for the ideal situation where a location l is reached only by those nodes which are interested in communicating with it.

Let us write $brd(P, l)$ for $brd(P, \{l\})$ (see definition above). Moreover, given a network M consisting of k devices:

$$M = n_1[P_1]^{\mu_1}_{l_1,r_1} \mid ... \mid n_k[P_k]^{\mu_k}_{l_k,r_k}$$

we write $brd(M, l)$ for

$$n_1[brd(P_1, l)]^{\mu_1}_{l_1,r_1} \mid ... \mid n_k[brd(P_k, l)]^{\mu_k}_{l_k,r_k}.$$

The next definition provides an efficient proof technique for the notion of Receiver-centered Interference.

Definition 14 (Absence of Receiver-centered Interference). *We say that a location l is free of* Receiver-centered Interference *with respect to a network M if,*

$$M \cong brd(M, l).$$

Notice that, by contextuality, if l is free of *Receiver-centered Interference* with respect to M then for any node n placed at location l, and for any radius r, mobility tag μ and process P, we have

$$n[P]^{\mu}_{l,r} \mid M \cong n[P]^{\mu}_{l,r} \mid brd(M, l).$$

If we are interested in proving the absence of Receiver-centered Interference for a location l in a network M, but relative to a specific set of nodes S, then we can proceed as follows. First, we split M in two sub-networks, $M = M_{in_S} \mid M_{out_S}$ where M_{in_S} consists of all the nodes in M belonging to S, while M_{out_S} contains all the other nodes in the network. Then, by contextuality, it is sufficient to prove that

$$M_{in_S} \cong brd(M_{in_S}, l).$$

Indeed, this implies that

$$n[P]^{\mu}_{l,r} \mid M_{in_S} \mid M_{out_S} \cong n[P]^{\mu}_{l,r} \mid brd(M_{in_S}, l) \mid M_{out_S}.$$

Theorem 13 (Absence of Reciver-centered Interference). *Given a network*

$$M \cong n_1[P_1]^{\mu_1}_{l_1,r_1} \mid ... \mid n_k[P_k]^{\mu_k}_{l_k,r_k}$$

and a location l, then if l is free of Receiver-centered Interference *with respect to M, it holds that $I_{rec}(l, M) = 0$.*

Proof. We will give a proof by contradiction. Since l is free of *Receiver-centered Interference* we can write:

$$n[P]^{\mu}_{l,r} \mid M \cong n[P]^{\mu}_{l,r} \mid snd(M)$$

for any n, P, l, r. In particular let consider $P \equiv c(v).P'$. Now suppose by contradiction that $I_{rec}(l, M) \neq 0$. Then there exists some $j \in [1 - k]$ such that $l \notin \texttt{rcv}(P_j) \wedge d(l_j, l) \leq r_j$. Since n_j is an active node, the process P_j will surely execute an output action with transmission radius r_j:

$$P_j \Longrightarrow c_{L,r_j}!\langle v\rangle.P'_j$$

Then, as l will receive the output of n_j (it is within its transmission range), we can write:

$$\begin{array}{l} n[P]^{\mu}_{l,r} \mid snd(M, l) \Longrightarrow \\ n[P]^{\mu}_{l,r} \mid n_1[snd(P_1, l)]^{\mu_1}_{l_1,r_1} \mid ...n_j[c_{L,r_j}!\langle v\rangle.P'_j]^{\mu_j}_{l_j,r_j}... \mid n_k[snd(P_k, l)]^{\mu_k}_{l_k,r_k} \xrightarrow{c!v@l} \\ n[P']^{\mu}_{l,r} \mid n_1[snd(P_1, l)]^{\mu_1}_{l_1,r_1} \mid ...n_j[P'_j]^{\mu_j}_{l_j,r_j}... \mid n_k[snd(P_k, l)]^{\mu_k}_{l_k,r_k} \end{array}$$

The same action cannot be performed by $n[P]^{\mu}_{l,r} \mid M$, by the initial hypothesis ($l \notin \texttt{rcv}(P_j)$). So we have reached the contradiction.

7 Conclusion

Ad hoc networks is a new area of mobile communication networks that has attracted significant attention due to its challenging problems. Many researchers have proposed formal models, such as process algebras, in order to reason on properties and problems of this kind of networks(see, e.g., [25, 10, 18, 20]).

The main goal of our work was to provide a formal model in order to reason about the problem of limiting the power consumption of communications. One of the most critical challenges in managing mobile Ad hoc networks is actually to find a good equilibrium between network connectivity and power saving. The ability of a node to control (and hence limit) the power of its transmission is represented by the introduction of a variable radius. Even though not all the devices have the ability of adjusting their transmission power, modern technologies are quickly evolving, and at the moment there already exist devices which enable

one to choose among two or more different power levels. For this reason many researches have proposed algorithms and protocols with the aim of providing a way to decide the best transmission power for a node's communication in a given environment (see, e.g., [5, 24]); other researches has been done in order to choose a fixed transmission range for the whole network (see, e.g.,[19]), in order to simplify the management of a MANET (a common transmission power will provide bidirectional links among the nodes).

One of the most important problem concerning a MANET's management is the choice of a good routing protocol, as the dynamic and precarious nature of this kind of network makes most of the routing protocols existing in literature not suitable for routes management (nodes can move arbitrarily within the network, changing continuously the topology and increasing the frequency of links breakage). In the recent years the problem of providing an efficient routing protocol has been faced together with the necessity of controlling power consumption of nodes' transmissions. Many researchers have proposed new power-aware routing protocols specifically developed for MANETs ([11, 28]), or modified some existing and commonly used routing protocols in order to reduce power consumption ([7, 1]).

In this paper we presented a calculus (E-BUM) which, by its characteristics of modelling broadcast, multicast and unicast communications, and the ability of a node to change its transmission power in accordance with the protocol it is executing, results to be a valid formal model for an accurate analysis, evaluation and comparison of the energy-aware protocols and algorithms specifically developed for Mobile ad hoc networks.

References

1. P. Bergamo, A. Giovanardi, A. Travasoni, D. Maniezzo, G. Mazzini, and M. Zorzi. Distributed Power Control for Energy Efficient Routing in Ad Hoc Networks. *Wireless Networks*, 10(1):29–42, 2004.
2. A. Bossi, R. Focardi, C. Piazza, and S. Rossi. Verifying Persistent Security Properties. *Computer Languages, Systems and Structures*, 30(3-4):231–258, 2004.
3. S. Bucchegger and J.Y. Le Boudec. Cooperative Routing in Mobile Ad-Hoc Networks: Current Efforts Against Malice and Selfishness. In *Proc. of Mobile Internet Workshop*, 2002.
4. M. Burkhart, P. von Rickenbach, R. Wattenhofer, and A. Zollinger. Does Topology Control Reduce Interference? In *Proc. of the 5th Symposium on mobile Ad-hoc Networking and Computing*, volume 623, pages 9–19. ACM, 2004.
5. T. Calamoneri, A. Clementi, A. Monti, G. Rossi, and R. Silvestri. Minimum-Energy Broadcast in Random-Grid Ad-Hoc Networks: Approximation and Distributed Algorithms. In *MSWiM '08: Proc. of the 11th Int. Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, pages 354–361, New York, NY, USA, 2008. ACM.
6. Ian D. Chakeres and E. M. Belding-Royer. Aodv Routing Protocol Implementation Design. In *Proc. of the 24th Int. Conference on Distributed Computing Systems Workshops - W7: EC (ICDCSW'04)*, volume 7, pages 698–703. IEEE press, 2004.
7. G. Ferrari, S. A. Malvassori, M. Bragalini, and O.K. Tonguz. Physical Layer-constrained Routing in Ad-hoc Wireless Networks: A Modified aodv Protocol with Power Control. In *Int. Workshop on Wireless Ad-Hoc Networks 2005 (IWWAN'05)*, 2005.
8. R. Focardi and S. Rossi. Information Flow Security in Dynamic Contexts. *Journal of Computer Security*, 14:65–110, 2006.
9. M. Fusen, R. Wattenhofer, and A. Zollinger. Interference Arises at the Receiver. In *Proc. of the Int. Conference on Wireless Networks, Communications, and Mobile Computing (WIRELESSCOM'05)*. IEEE press, 2005.
10. J.C. Godskesen. A Calculus for Mobile Ad Hoc Networks. In *Proc. of the 10th Int. Conference on Coordination Models and Languages (COORDINATION'07)*, volume 3653 of *LNCS*, pages 132–150. Springer-Verlag, Berlin, 2007.
11. J. Gomez and A. T. Campbell. Conserving Transmission Power in Wireless Ad Hoc Networks. In *ICNP*, pages 11–14, 2001.
12. J. Goubault-Larrecq, C. Palamidessi, and A. Troina. A Probabilistic Applied Pi-Calculus. *Lecture Notes in Computer Science*, 4807/2009:175–190, 2007.
13. J. Hillston. *A Compositional Approach to Performance Modelling*. Cambridge University Press, 1996.
14. M. Merro. An Observational Theory for Mobile Ad Hoc Networks. *Information and Computation*, 207(2):194–208, 2009.
15. F. Meyer auf de Heide, C. Schindelhauer, K. Volbert, and M. Grünewald. Energy, Congestion and Dilation in Radio Networks. In *Proc. of the 14th Annual ACM Symposium on Parallel Algorithms and Architectures (SPAA'02)*, pages 230–237. ACM, 2002.
16. R. Milner. *Communication and Concurrency*. Prentice-Hall, 1989.
17. R. Milner. *Communicating and Mobile Systems: the Pi-Calculus*. Cambridge University Press, 1999.
18. S. Nanz and C. Hankin. A Framework for Security Analysis of Mobile Wireless Networks. *Theoretical Computer Science*, 367(1):203 – 227, 2006.

19. S. Narayanaswamy, V. Kawadia, R. S. Sreenivas, and P. R. Kumar. Power Control in Ad Hoc Networks : Theory, Architecture, Algorithm and Implementation of the compow Protocol. In *European Wireless Conference*, 2002.
20. K. V. S. Prasad. A Calculus of Broadcasting Systems. *Science of Computer Programming*, 25(2-3):285–327, 1995.
21. V.N. Raghavan, T.P.M. Labbai, N. Bhalaji, and S. Kesavan. Extended Dynamic Source Routing Protocol for the Non Co-operating Nodes in Mobile Ad-hoc Networks. *Int. Journal of Applied Mathematics and Computer Sciences*, 3(1):12–17, 2007.
22. R.Milner and D. Sangiorgi. Barbed Bisimulation. In *Proc. of the Int. Colloquium on Automata, Languages and Programming (ICALP'92)*, volume 623 of *LNCS*, pages 685–695. Springer-Verlag, Berlin, 1992.
23. E. M. Royer and C. E. Perkins. Multicast Operation of the Ad-Hoc On-demand Distance Vector Routing Protocol. *Proc. of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, pages 207–2018, 1999.
24. M. Sanchez, P. Manzoni, and Z. J. Haas. Determination of Critical Transmission Range in Ad-Hoc Networks. In *Proc. of the Multiaccess, Mobility and Teletraffic for Wireless Communications (MMT) Conference*, 1999.
25. A. Singh, C.R. Ramakrishnan, and S.A. Smolka. A Process Calculus for Mobile Ad Hoc Networks. In *Proc. of the 10th Int. Conference on Coordination Models and Languages (COORDINATION'08)*, volume 5052 of *LNCS*, pages 296–314. Springer-Verlag, Berlin, 2008.
26. Andrew S. Tanenbaum. *Computer Networks*. Prentice Hall, 2003.
27. P. von Rickenbach, S. Schmid, R. Wattenhofer, and A. Zollinger. A Robust Interference Model for Wireless Ad-Hoc Networks. In *5th Int. Workshop on Algorithms for Wireless, Mobile, Ad Hoc and Sensor Networks (WMAN)*. IEEE press, 2005.
28. N. Wang, J. Chen, Y. Huang, and Y. Su. A Power-Aware Multicast Routing Protocol for Mobile Ad Hoc Networks with Mobility Prediction. *Wireless Pers. Comm.*, 43:1479–1497, 2007.
29. Ieee 802.11 official website. http://www.ieee802.org/11.
30. L. Zhou and Z.J. Haas. Securing Ad Hoc Networks. *IEEE Network Magazine*, 1999.