Probabilistic Mobility Models for Mobile and Wireless Networks

Lei Song, Jens Chr. Godskesen

Probabilistic Mobility Models for Mobile and Wireless Networks[⋆]

Lei Song and Jens Chr. Godskesen

IT University of Copenhagen
Rued Langgaards Vej 7
DK-2300 Copenhagen S, Denmark
{leis,jcg}@itu.dk

Abstract. In this paper we present a probabilistic broadcast calculus for mobile and wireless networks whose connections are unreliable. In our calculus, broadcasted messages can be lost with a certain probability, and due to mobility the connection probabilities may change. If a network broadcasts a message from a location, it will evolve to a network distribution depending on whether nodes at other locations receive the message or not. Mobility of nodes is not arbitrary but guarded by a *probabilistic mobility function* (PMF), and we also define the notion of a weak bisimulation given a PMF. It is possible to have weak bisimular networks which have different probabilistic connectivity information. We furthermore examine the relation between our weak bisimulation and a minor variant of PCTL* [1]. Finally, we apply our calculus on a small example called the Zeroconf protocol [2].

1 Introduction

Mobile and wireless networks have gained in popularity in recent years, and the application area is broad, spanning from ambient intelligence, wireless local area networks, sensor networks, and cellular networks for mobile telephony. The key communication primitive in wireless communication is message broadcast but, differently from wired local area networks, broadcast in wireless networks is *local*, hence only nodes within the communication range of the emitting node can receive the message, and due to mobility the communication area may change over time.

Mobility and local wireless broadcast has been studied in the calculi: CBS♯[3], the ω-calculus[4], CMN[5], RBPT[6], and CMAN[7, 8]. All these calculi only deal with connectivity in two modes: either two nodes are connected or disconnected. It is often assumed that when a node at location l is within the transmission range of another node at location k, then the node at l can receive messages broadcasted from k with probability 1, otherwise with probability 0. Here we refine this assumption and equip a connection with a probability, since in an unreliable medium we cannot guarantee that the broadcasted messages will always be received even within the transmission range. For example, in Fig. 1 the dashed circle denotes the transmission range of k, every node at a location within the circle, such as l and m, may receive the messages broadcasted

[⋆] Supported by the VKR Centre of Excellence MT-LAB

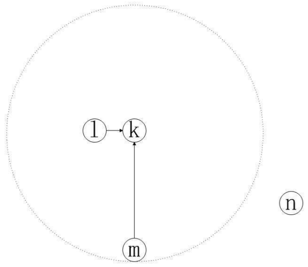

Fig. 1. Connectivity example.

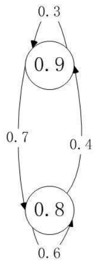

Fig. 2. Equivalent connection probabilities.

from k, but the node at n outside the circle cannot. Intuitively, although both l and m are in the transmission range of k, it is more reasonable to let nodes there receive messages from k with different probabilities since m is further away from k than l. In our calculus, the connectivity of this network can be denoted as $\{\{(0.9, l), (0.5, m), (0, n)\} \longmapsto k\}$ if nodes at l, m, n can receive messages from k with probability 0.9, 0.5, and 0 respectively.

In order to model mobility we let connection probabilities between locations change, and the changes are also probabilistic. For instance, the nodes at location m in Fig. 1 may move closer to location k with a certain probability in which case the nodes at m will be able to receive messages from k with a higher probability.

In practice, when verifying properties of a mobile network it will be reasonable to assume that mobility within a network is not arbitrarily but respects certain rules or distributions. Therefore we introduce a *probabilistic mobility function* (PMF) which defines the mobility rules of all the connections. A PMF returns the probability for a connection evolving from one value into another. For example, if in a PMF the connection probability from l to k is given by Fig. 2, then we know that it can change to 0.8 with probability 0.7 or stay at 0.9 with probability 0.3, that is:

$$\{\{(0.9, l), (0.5, m), (0, n)\} \longmapsto k\} \longrightarrow \begin{cases} 0.7 : \{\{(0.8, l), (0.5, m), (0, n)\} \longmapsto k\} \\ 0.3 : \{\{(0.9, l), (0.5, m), (0, n)\} \longmapsto k\} \end{cases}$$

Hence we equip mobility with probabilities, and after each mobility action the network will evolve into a distribution with the probabilities specified by the given PMF. We expect that usually a PMF can be obtained based on measurement of case studies.

Our network calculus consists of concurrent processes (nodes) communicating internally over channels at (logical) locations and broadcasting messages to processes at neighboring locations over probabilistic connections that may change probabilistically over time as outlined above. The semantics is a combination of probability, concurrency, and non-determinism. Formally the labeled transition system semantics gives rise to a *simple probabilistic automata* as outlined in [9], which allows us to use a labeled variant of PCTL*[1] to reason about properties of networks specified in our calculus. We also define a (weak) bisimulation along the lines of [1] and show that it is sound and complete for our version of PCTL*. In our bisimulation, we abstract from mobility as in the other calculi for mobile and wireless systems mentioned above.

As a novelty a bisimulation is parameterized by a PMF, and since we abstract from mobility we consider two probabilities of a connection to be equivalent if they can evolve into each other eventually with probability 1 after a number of mobility steps. Intuitively, it means that a connection due to mobility can take any of the equivalent probabilities. For example, given the PMF in Fig. 2 the state 0.8 can evolve into 0.9 with probability 1 after an infinite number of steps. Furthermore, two locations l and m are considered equivalent if any other location k is connected to them by equivalent probabilities, because then nodes at k can with probability 1 receive messages from l and m with the same probability.

Another important contribution is the introduction of *unknown probabilities*. Since we are dealing with open systems where contexts may contain new nodes and information about connection probabilities, we cannot in a network expect to know the probability of all possible connections. We integrate unknown probabilities in our theory to deal with these cases. Intuitively a connection with an unknown probability means that the probability for the connection can be any value.

The paper is organized as follows: the syntax of our calculus is presented in the next section and in Section 3 we give the Labeled Transition System for it. In Section 4 a weak bisimulation is defined and we also prove it to be a congruence. PCTL* and its relation with weak bisimulation is given in Section 5. We illustrate the application of our calculus with a simple protocol called Zeroconf in Section 6. Finally, we end by a conclusion and future works.

2 The Calculus

Before introducing our calculus, we first give the following general definitions. A *probability space* is a triplet $\mathcal{P} = (\Omega, F, \eta)$ where Ω is a set, F is a collection of subsets of Ω closed under complement and countable union that includes Ω. $\eta : F \to [0,1]$ is a probability distribution such that $\eta(\Omega) = 1$, and for any collection $\{C_i\}_i$ of at most countably many pairwise disjoint elements of F, $\eta(\cup_i C_i) = \sum_i \eta(C_i)$. A probability space (Ω, F, η) is discrete if Ω is countable and $F = 2^{\Omega}$, and hence abbreviated as (Ω, η). Given probability spaces $\{\mathcal{P} = (\Omega_i, \eta_i)\}_{i\in I}$ and weights $w_i > 0$ for each i such that $\sum_{i\in I} w_i = 1$, the *convex combination* $\sum_{i\in I} w_i \mathcal{P}_i$ is defined as the probability space (Ω, η) such that $\Omega = \bigcup_{i\in I} \Omega_i$ and for each set $Y \subseteq \Omega$, $\eta(Y) = \sum_{i\in I} w_i \eta_i(Y \cap \Omega_i)$. We let $\{\rho_i : N_i\}_{i\in I}$ denote the discrete probability space $(\{N_{i\in I}\}, \eta)$ where $\eta(\{N_i\}) = \rho_i$.

We presuppose a countably infinite set N of names, ranged over by x, y, z and a finite set L of location names, ranged over by k, l, m, n. The variables $\tilde{k}, \tilde{l} \ldots$ are used to denote a set of locations. In addition, we also suppose a finite set of probabilities $\wp$ including 0 and 1 ranged over by $\rho, \rho', \rho_1 \ldots$. We define a *location connection set*, ranged over by $\mathbb{L}, \mathbb{K} \ldots$, as a subset of $\{(\rho, l) \mid \rho \in \wp, l \in L\}$. We use $l(\mathbb{L}) = \{l \mid (\rho, l) \in \mathbb{L}\}$ to denote all the locations in $\mathbb{L}$. The syntax of processes is defined by the following grammar:

$$p, q ::= 0 \quad | \quad Act.p \quad | \quad \text{if } (x = y) \text{ then } p \text{ else } q \quad | \quad \nu x p \quad | \quad p \| q \quad | \quad !p$$

$$Act ::= \langle x \rangle \quad | \quad \bar{y}\langle x \rangle \quad | \quad (x) \quad | \quad y(x)$$

Action $\langle x \rangle$ represents broadcasting a message x, while the reception of a broadcasted message is denoted by (x); $\bar{y}\langle x \rangle$ denotes sending a message x via the channel y and in

Table 1. Structural congruence.

$\lfloor 0 \rfloor_l \equiv 0$	$\lfloor !p \rfloor_l \equiv \lfloor p \| !p \rfloor_l$	$\nu x E \| E' \equiv \nu x (E \| E'),$ if $x \notin fn(E')$
$E \| 0 \equiv E$	$\lfloor p \| q \rfloor_l \equiv \lfloor p \rfloor_l \| \lfloor q \rfloor_l$	$\lfloor \text{if } (x = x) \text{ then } p \text{ else } q \rfloor_l \equiv \lfloor p \rfloor_l$
$\lfloor \nu x.p \rfloor_l \equiv \nu x \lfloor p \rfloor_l$	$(E \| E') \| E'' \equiv E \| (E' \| E'')$	$\lfloor \text{if } (x = y) \text{ then } p \text{ else } q \rfloor_l \equiv \lfloor q \rfloor_l, x \neq y$
$\nu x \nu y E = \nu y \nu x E$	$E \| F \equiv F \| E$	$\{\mathbb{L}_1 \longmapsto k\} \| \{\mathbb{L}_2 \longmapsto k\} \equiv \{\mathbb{L}_1 \cup \mathbb{L}_2 \longmapsto k\}, l(\mathbb{L}_1) \cap l(\mathbb{L}_2) = \emptyset$

contrast $y(x)$ represents receiving a message x on channel y. Process 0 is the deadlocked process; $Act.p$ is the process that can perform action Act and then behave as p; if $(x = y)$ then p else q behaves as p if names x and y match and as q otherwise; νxp means that name x is bounded in the process p; in composition $p||q$, the processes p and q can proceed in parallel and can also interact via shared names; $!p$ means an unbounded number of parallel compositions of process p. As usual we often leave out a trailing 0.

The set of networks $\mathcal{N}$ is defined by the grammar:

$$E, F ::= 0 \quad | \quad \lfloor p \rfloor_l \quad | \quad \{\mathbb{L} \longmapsto l\} \quad | \quad \nu x E \quad | \quad E||F$$

Here $\lfloor p \rfloor_l$ is a process p at location l; $\nu x E$ and $E||F$ are restriction and parallel composition respectively which have the standard meaning; $\{\mathbb{L} \longmapsto l\}$ denotes connection information, i.e. if $(\rho, k) \in \mathbb{L}$, the node at location k is connected to l and can receive messages from l with probability ρ. We use $E, F, G \ldots$ to range over $\mathcal{N}$.

We define a *network distribution* as a probability space $\mathbb{E} = \{(\rho_i : E_i)\}_{i \in I}$ meaning that a network can evolve into E_i with probability ρ_i. We use $\mathbb{E}, \mathbb{F}, \mathbb{G} \ldots$ to range over network distributions ND. If a network distribution consists of a single network, such as $\{(1 : E)\}$, then we denote it as E directly. Parallel composition of network distributions is defined by:

$$\mathbb{E}||\mathbb{F} = \{(\rho \times \rho' : E||F) \mid (\rho : E) \in \mathbb{E}, (\rho' : F) \in \mathbb{F}\}$$

A substitution $\{y/x\}$ can be applied to a node, network or network distribution. When applied to a network distribution, it means applying this substitution to each network within this distribution. The set of free names and bound names in E, denoted by $fn(E)$ and $bn(E)$ respectively, are defined as expected. Structural congruence, $\equiv$, is the least equivalence relation and congruence closed by the rules in Table 1 and α-conversion. $\equiv$ is extended to network distributions as expected.

In the following, we use $\rho_{k \longmapsto l}$ as an abbreviation of the probability from which k can receive messages from l. As mentioned, we assume that mobility is not arbitrary but respects certain rules. These rules are given by a function $pf : L \times L \times \wp \times \wp \rightarrow \wp$ called a *probabilistic mobility function* (PMF), the probability for $\rho_{k \longmapsto l}$ changing from ρ to ρ' is given by $pf(k, l, \rho, \rho')$. Let $G^{pf}_{k \longmapsto l}$ be the underlying directed graph for $\rho_{k \longmapsto l}$ given pf, where vertices are possible values of $\rho_{k \longmapsto l}$ and where there is an edge from state ρ to ρ' iff $pf(k, l, \rho, \rho') \in (0, 1]$, and we ignore nodes with 0 in-degree and 0 out-degree. Without causing any confusion, sometimes we also use $G^{pf}_{k \longmapsto l}$ to denote the set of nodes in the graph called the *support* of $\rho_{k \longmapsto l}$. A PMF pf is valid if for all $G^{pf}_{k \longmapsto l}$, $G^{pf}_{k \longmapsto l} \neq \emptyset$ and for each $\rho \in G^{pf}_{k \longmapsto l}$, $\sum_{\rho' \in G^{pf}_{k \longmapsto l}} pf(k, l, \rho, \rho') = 1$. In the following, we only consider valid PMFs.

A *well-formed network* under a given *pf* is defined inductively by: 0 and $\lfloor p \rfloor_l$ are well-formed, and $\nu x E$ is well-formed if E is well-formed; $\{\mathbb{L} \longmapsto l\}$ is well-formed if all location names in $\mathbb{L}$ are distinct and for each $(\rho, k) \in \mathbb{L}$, $\rho \in G^{pf}_{k \longmapsto l}$; $E \| F$ is well-formed if both E, F are well-formed and for any $l, k \in L$ with $l \neq k$, there does not exist E', F' such that $E \equiv \{\{(\rho, k)\} \longmapsto l\} \| E'$ and $F \equiv \{\{(\rho', k)\} \longmapsto l\} \| F'$. In the sequel given a *pf* we only consider the set of well-formed networks $\mathcal{N}_{pf}$. We assume that every node can receive messages broadcasted by itself with probability 1, but for simplicity we often denote this implicitly.

We use $\rho_{k \longmapsto l}(E)$ to denote the connection probability from k to l in network E, when the requested probability occurs in E it returns this value otherwise it returns $\theta_{k \longmapsto l}$ to denote an *unknown probability*, i.e.

$$\rho_{k \longmapsto l}(E) = \begin{cases} \rho & \text{if there exists } E^{'} \text{ s.t. } E \equiv \{\mathbb{L} \longmapsto l\} \| E^{'} \text{ and } (\rho, k) \in \mathbb{L} \\ \theta_{k \longmapsto l} & \text{otherwise} \end{cases}$$

We use $\mathfrak{D}_l(E)$ to denote the set of all connection probabilities from some locations to l in E, that is $\mathfrak{D}_l(E)$ is the smallest set such that $(\rho_{k \longmapsto l}(E), k) \in \mathfrak{D}_l(E)$ if $\rho_{k \longmapsto l}(E) \in \wp$.

We generalize network distributions to contain unknown probabilities. Let $\hat{\theta}_{k \longmapsto l}$ denote $\theta_{k \longmapsto l}$ or $1 - \theta_{k \longmapsto l}$. We let ρ range over *generalized probabilities*, i.e. expressions being a finite sequence $\hat{\theta}_{k_0 \longmapsto l_0} \times ... \times \hat{\theta}_{k_i \longmapsto l_i} \times \rho$. We say that a generalized probability $\hat{\theta}_{k_0 \longmapsto l_0} \times ... \times \hat{\theta}_{k_i \longmapsto l_i} \times \rho$ is 0 if $\rho = 0$. A *generalized network distribution*, GND, is defined inductively as follows: A network distribution is a GND, if $\mathbb{G} = \{(\rho_i : E_i)\}_{i \in I}$ is a GND then $(\theta_{k \longmapsto l} \times \mathbb{G}) + ((1 - \theta_{k \longmapsto l}) \times \mathbb{G}) = \{(\theta_{k \longmapsto l} \times \rho_i : E_i), (1 - \theta_{k \longmapsto l} \times \rho_i : E_i)\}_{i \in I}$ is a GND. We may substitute unknown probabilities in a GND with known probabilities, e.g. $\mathbb{E} \circ \mathfrak{D}_l(E)$ means replacing each unknown probability $\theta_{k \longmapsto l}$ in $\mathbb{E}$ with the known probability $\rho_{k \longmapsto l}(E)$ if $(\rho_{k \longmapsto l}(E), k) \in \mathfrak{D}_l(E)$.

3 Label Transition System

In this section we introduce the labeled transition system semantics for our calculus; the semantics is parameterized by a given PMF which is denoted by *pf* and left implicit throughout the rest of this section.

First we define a set of actions $\mathcal{A}$, ranged over by α, by:

$$\alpha ::= \nu\tilde{x}\langle x, \mathbb{K}\rangle@l \mid (x, \mathbb{K}) \triangleleft l \mid \nu\tilde{x}\bar{y}\langle x\rangle@l \mid y(x)@l \mid \tau$$

$\nu\tilde{x}\langle x, \mathbb{K}\rangle@l$ denotes that a node at location k receives the message x broadcasted from l with probability ρ if $(\rho, k) \in \mathbb{K}$; $(x, \mathbb{K}) \triangleleft l$ means that the node at location k receives the message x from location l with probability ρ if $(\rho, k) \in \mathbb{K}$; $\nu\tilde{x}\bar{y}\langle x\rangle@l$ means sending x on channel y at the location l (i.e.unicast), on the contrary $y(x)@l$ means that x can be received on the channel y at location l. $\tilde{x}$ is either a singleton set $\{x\}$ or empty, if $\tilde{x}$ is empty then x is free else it is bounded.

The labeled transition system is defined in Table 2; notice that the semantics is late, i.e. the bound names of an input become instantiated only when inferring a communication. Rules *out*, *in*, *com*, *par*, *res*, *open*, *str* are either standard or trivial and need no more comments; *brd* means that a process at a location can broadcast a message to the

Table 2. Labeled transition system.

$$\text{(par)}\,\frac{E \xrightarrow{\alpha} \mathbb{E}}{E \| F \xrightarrow{\alpha} \mathbb{E} \| F} \quad \alpha \notin ((x) \triangleleft l, \nu\tilde{x}\langle x\rangle @ l), bn(\alpha) \cap fn(F) = \emptyset$$

$$\text{(out)}\,\frac{}{\lfloor \bar{y}\langle x\rangle.p\rfloor_l \xrightarrow{\bar{y}\langle x\rangle @ l} \lfloor p\rfloor_l} \qquad \text{(open)}\,\frac{E \xrightarrow{\alpha} \mathbb{E}'}{\nu x E \xrightarrow{\nu x \alpha} \mathbb{E}'} \quad \alpha \in \{\bar{y}\langle x\rangle @ l, \langle x\rangle @ l\}, x \neq y$$

$$\text{(in)}\,\frac{}{\lfloor y(x).p\rfloor_l \xrightarrow{y(x) @ l} \lfloor p\rfloor_l} \qquad \text{(com)}\,\frac{E \xrightarrow{\nu\tilde{z}\bar{y}\langle z\rangle @ l} E' \quad F \xrightarrow{y(x) @ l} F'}{E \| F \xrightarrow{\tau} \nu\tilde{z}(E' \| F'\{z/x\})} \quad \tilde{z} \cap fn(F) = \emptyset$$

$$\text{(res)}\,\frac{E \xrightarrow{\alpha} \mathbb{E}'}{\nu x E \xrightarrow{\alpha} \nu x \mathbb{E}'} \quad x \notin n(\alpha) \qquad \text{(pro)}\,\frac{}{\{\mathbb{K} \longmapsto k\} \xrightarrow{(x,\mathbb{K}) \triangleleft k} \{\mathbb{K} \longmapsto k\}}$$

$$\text{(los)}\,\frac{}{\lfloor Act.p\rfloor_k \xrightarrow{(x,\emptyset) \triangleleft l} \lfloor Act.p\rfloor_k} \quad Act \neq (y) \text{ and } x \notin fn(\lfloor Act.p\rfloor_k)$$

$$\text{(rec1)}\,\frac{}{\lfloor (x).p\rfloor_k \xrightarrow{(x,\emptyset) \triangleleft l} \{(\theta_{k \longmapsto l} : \lfloor p\rfloor_k), (1 - \theta_{k \longmapsto l} : \lfloor (x).p\rfloor_k)\}}$$

$$\text{(brd)}\,\frac{}{\lfloor \langle x\rangle.p\rfloor_l \xrightarrow{\langle x,\emptyset\rangle @ l} \lfloor p\rfloor_l} \qquad \text{(rec2)}\,\frac{E \xrightarrow{(x,\mathbb{L}) \triangleleft l} \mathbb{E} \quad F \xrightarrow{(x,\mathbb{K}) \triangleleft l} \mathbb{F}}{E \| F \xrightarrow{(x,\mathbb{L} \cup \mathbb{K}) \triangleleft l} (\mathbb{E} \circ \mathfrak{D}_l(F)) \| (\mathbb{F} \circ \mathfrak{D}_l(E))}$$

$$\text{(syn)}\,\frac{E \xrightarrow{\nu\tilde{y}\langle y,\mathbb{L}\rangle @ l} \mathbb{E} \quad F \xrightarrow{(x,\mathbb{K}) \triangleleft l} \mathbb{F}}{E \| F \xrightarrow{\nu\tilde{y}\langle y,\mathbb{L} \cup \mathbb{K}\rangle @ l} ((\mathbb{E} \circ \mathfrak{D}_l(F)) \| (\mathbb{F}\{y/x\} \circ \mathfrak{D}_l(E)))} \quad \tilde{y} \cap (\{x\} \cup fn(F)) = \emptyset$$

$$\text{(con)}\,\frac{}{\{\{(\rho, l)\} \longmapsto k\} \xrightarrow{\tau} \{pf(l,k,\rho,\rho') : \{\{(\rho', l)\} \longmapsto k\}\}} \qquad \text{(str)}\,\frac{E \equiv F \xrightarrow{\alpha} \mathbb{F} \equiv \mathbb{E}}{E \xrightarrow{\alpha} \mathbb{E}}$$

network it belongs to; *rec*1 states that nodes might evolve with unknown probability when they are ready to receive messages; *rec*2 allows to combine two networks which can receive a broadcasted message in parallel, and notice that unknown probabilities may be substituted by known ones. The union $\mathbb{L} \cup \mathbb{K}$ denotes that in a parallel composition the message can arrive at locations in both $\mathbb{L}$ and $\mathbb{K}$ with specific probabilities; *syn* deals with synchronization and broadcast, in that a network can broadcast a message to any neighbor network where each location may receive with a certain probability. For the same reason as in *rec*2, the location connection set in the resulting action is the union of the two location connection sets in the synchronizing actions. Notice that some processes must discard broadcasted messages as explained by the rules *los*.

In the rules *rec*2 and *syn*, we have that when parallelizing two networks, they can get connection information from each other and update the correspondent unknown probabilities. Note here that when there is a message broadcasted from l, we only need to update possibly unknown probabilities with probabilities from connections to l, that is why we only need $\mathcal{D}_l(E)$ and $\mathcal{D}_l(F)$ to update the unknown probabilities in *rec*2 and *syn*. The rule *con* changes the connection probabilities in a network depending on the

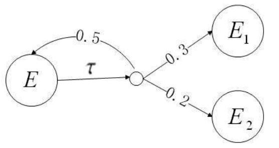

Fig. 3. A mobility transition.

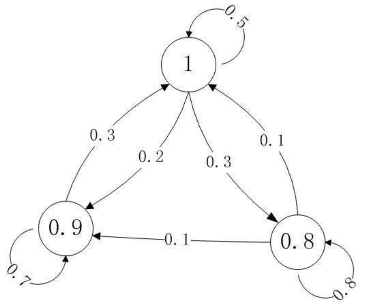

Fig. 4. A bottom strongly connected component.

PMF parameterizing the semantics, and the rule *pro* contributes by revealing the current probabilistic connectivity information.

Example 1. Suppose we have a network E with $\rho_{l\longmapsto k}(E) = 0.8$ and we also know from the given PMF pf that $pf(l, k, 0.8, 0.9) = 0.3$, $pf(l, k, 0.8, 0.7) = 0.2$ and $pf(l, k, 0.8, 0.8)$ $= 0.5$, then we have the derivation in Fig. 3 with $\rho_{l\longmapsto k}(E_1) = 0.9$, $\rho_{l\longmapsto k}(E_2) = 0.7$.

4 Weak Bisimulation

In this section we provide a weak bisimulation for our calculus.

A broadcast action, $\langle x, \mathbb{K}\rangle@l$, contains the name of the broadcasting location, the broadcasted message, and a location connection set which denotes locations receiving the message with specific probabilities. We want to allow a network to simulate such an action by $\langle x, \mathbb{K}\rangle@m$, if l and m are *mobility equivalent*. Intuitively, two locations are mobility equivalent if any of their connection probabilities, say $\rho_{k\longmapsto l}$ and $\rho_{k\longmapsto m}$, are able to evolve into each other eventually with probability 1, in which case the node at location k can with probability 1 receive messages from l and m with the same probability. For example, if the mobility of $\rho_{k\longmapsto l} = 0.8$ and $\rho_{k\longmapsto m} = 0.9$ is given by Fig. 4, then $\rho_{k\longmapsto l}$ can evolve into $\rho_{k\longmapsto m}$ and vice versa. Otherwise, if the mobility of $\rho_{k\longmapsto l} = 0.6$ and $\rho_{k\longmapsto m} = 0.5$ is given by Fig. 5 then $\rho_{k\longmapsto m}$ may evolve into $\rho_{k\longmapsto l}$ but not the other way around.

The following definitions are used to define mobility equivalence between two locations in their respective networks.

A subgraph SG of $G^{pf}_{l\longmapsto k}$ is called *strongly connected* if for each pair (ρ, ρ') of states in SG there exists a path fragment $\rho_0\rho_1 \ldots \rho_i$ such that $\rho_j \in SG$ and $pf(l, k, \rho_j, \rho_{j+1}) > 0$ for $0 \leq j < i$ with $\rho = \rho_0$ and $\rho' = \rho_i$. A *strongly connected component* (SCC) denotes a strongly connected set of states such that no proper superset of it is strongly connected. A *bottom* SCC (BSCC) is an SCC from which no state outside this SCC is reachable. If probabilities are in the same BSCC, they can for sure evolve into each other, or in probabilistic terms they can evolve into each other eventually with probability 1. For example, Fig. 4 is a BSCC whereas Fig. 5 and 6 are not. If two probabilities ρ and ρ' are in the same BSCC within $G^{pf}_{l\longmapsto k}$, then we write $pf(l, k, \rho, \rho')^* = 1$.

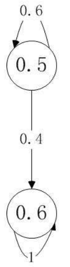

Fig. 5. A non-SCC.

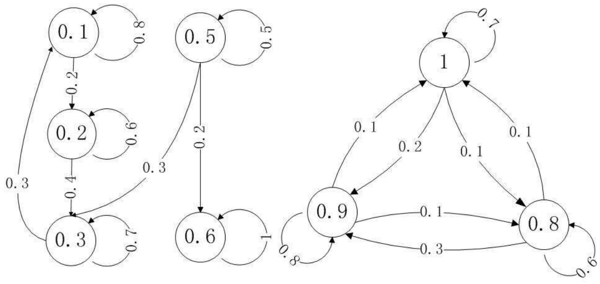

Fig. 6. A non-BSCC.

The *eventual support* of $\rho_{l\longmapsto k}$ under a given PMF pf, denoted by $ES^{pf}(l,k)$, is the set of all nodes (probabilities) which belong to a BSCC in $G^{pf}_{l\longmapsto k}$.

Definition 1. *$ES^{pf}(l,k)$ is consistent if $G^{pf}_{l\longmapsto k}$ is a BSCC.*

In the following, we use $[\![\rho]\!]_{ES^{pf}(l,k)}$ to denote the set of nodes of the BSCC of $G^{pf}_{l\longmapsto k}$ which contains the node ρ if $\rho \in ES^{pf}(l,k)$, here $[\![\theta_{l\longmapsto k}]\!]_{ES^{pf}(l,k)} = ES^{pf}(l,k)$ if $ES^{pf}(l,k)$ is consistent, otherwise $[\![\theta_{l\longmapsto k}]\!]_{ES^{pf}(l,k)} = \{\theta_{l\longmapsto k}\}$.

Definition 2. *Let pf be a PMF, then l in E and m in F are* mobility equivalent*, denoted by $l_E \asymp^{pf} m_F$, if for any $k \in L$, either i) $l = m$ with $\rho_{k\longmapsto l}(E) = \rho_{k\longmapsto m}(F)$, or ii) $\rho_{k\longmapsto l}(E) \in ES^{pf}(k,l) \cup \{\theta_{k\longmapsto l}\}$ and $\rho_{k\longmapsto m}(F) \in ES^{pf}(k,m) \cup \{\theta_{k\longmapsto m}\}$ such that $[\![\rho_{k\longmapsto l}(E)]\!]_{ES^{pf}(k,l)} = [\![\rho_{k\longmapsto m}(F)]\!]_{ES^{pf}(k,m)}$.*

That is, two locations l and m in E and F respectively are mobility equivalent if either a) the locations are identical and all other locations are connected to them in E and F with the the same (possibly unknown) connection probabilities, b) the probability for a connection to l belongs to a BSCC and the probability for the similar connection to m belongs to a BSCC with the same probabilities, if the probability for the connection to m is unknown in F, the eventual support for the connection must be consistent, or c) the probability for a connection to l is unknown in E, the eventual support ES for the connection is consistent, and the probability for the corresponding connection to m belongs to a BSCC with the same values as in ES. Intuitively, for the cases b) and c) it means that even though the connection probabilities for connections to l and m are not the same, then they eventually with probability 1 can evolve into each other by a number of mobility steps.

Example 2. Suppose the mobility rules for $\rho_{l\longmapsto k}$ and $\rho_{m\longmapsto k}$ are given by Fig. 6 and 4 respectively and let all other connection probabilities be permanently 1. Assume we are given two networks E and F such that $\rho_{l\longmapsto k}(E) = 0.9$, $\rho_{m\longmapsto k}(F) = \theta_{m\longmapsto k}$. Then $l_E \asymp^{pf} m_F$, but if $\rho_{l\longmapsto k}(E) = 0.3$ then $l_E \not\asymp^{pf} m_F$, since there is no way for $\rho_{m\longmapsto k}(F)$ to become 0.3.

It follows immediately from the definition of $\asymp^{pf}$ that it is an equivalence relation. Observe also that whenever $ES^{pf}(l,k)$ is consistent, then the unknown connection probability $\theta_{l\longmapsto k}$ can be assigned with any value in $ES^{pf}(l,k)$ while still preserving mobility equivalence.

In our weak bisimulation equivalence, we as usual abstract from internal steps which in our case also involve the probabilistic mobility steps changing connection probabilities. In order to capture that a connection probability for sure (with probability 1) can evolve into another, we introduce the relation $\rightarrow$. Let $\rightarrow$ be the least relation closed by parallel composition, restriction and structural congruence and such that $\{\{(\rho, l)\} \longmapsto k\} \rightarrow \{\{(\rho', l)\} \longmapsto k\}$ if $pf(l, k, \rho, \rho')^* = 1$.

We use $E \overset{\alpha}{\Longrightarrow} \mathbb{E}$ to denote that a distribution $\mathbb{E}$ is reached through a finite sequence of steps some of which are internal. Formally $\overset{\alpha}{\Longrightarrow}$ is the least relation such that, $E \overset{\alpha}{\Longrightarrow} \mathbb{E}$ iff (i) $\alpha = \tau$ and $E = \mathbb{E}$, (ii) $\alpha = \tau$ and $E \rightarrow \mathbb{E}$, or (iii) there exists a step $E \xrightarrow{\beta} \mathbb{E}'$ such that $\mathbb{E} = \sum_{(\rho:E')\in\mathbb{E}'} \rho\mathbb{E}_{E'}$, where $E' \overset{\tau}{\Longrightarrow} \mathbb{E}_{E'}$ if $\beta = \alpha$, otherwise $E' \overset{\alpha}{\Longrightarrow} \mathbb{E}_{E'}$ and $\beta = \tau$.

Since there might occur unknown probabilities during the evolution of networks, we have to resolve this in order to define our bisimulation. For that we introduce a set of networks denoted by Σ^{pf} and ranged over by σ^{pf}. The networks in Σ^{pf} only contain connection information for a given pf and it is defined by:

$$\Sigma^{pf} = \{ \mathop{\|}_{l\in L} \{\{(\rho, k) \mid k \in L\} \longmapsto l\} \mid \rho \in G^{pf}_{k\longmapsto l}\}$$

We write $E \bullet \sigma^{pf}$ to denote a network behaving like E but obtaining new connection information from σ^{pf}, that is,

$$E \bullet \{\emptyset \longmapsto l\} = E$$

$$E \bullet \{\{(\rho, k)\} \cup \mathbb{L} \longmapsto l\} = \begin{cases} E \bullet \{\mathbb{L} \longmapsto l\} & \rho_{k\longmapsto l}(E) \neq \theta_{k\longmapsto l} \\ (E \| \{\{(\rho, k)\} \longmapsto l\}) \bullet \{\mathbb{L} \longmapsto l\} & \mathit{otherwise} \end{cases}$$

The importance of mobility equivalence can be illustrated by the following lemma.

Lemma 1. *For each $\sigma^{pf} \in \Sigma^{pf}$, if $E \bullet \sigma^{pf} \xrightarrow{(x,\mathbb{K})\triangleleft l} \mathbb{E}$ and $l_E \asymp^{pf} m_E$ then $E \bullet \sigma^{pf} \overset{(x,\mathbb{K})\triangleleft m}{\Longrightarrow} \mathbb{E}$.*

We lift the notion of equivalence relation to distributions in the usual way.

Definition 3. *Let $\mathcal{R}$ be an equivalence relation over $\mathcal{N}_{pf}$. Two (non-generalized) network distributions $\mathbb{E}_1 = (\mathcal{N}_{pf}, \eta_1)$ and $\mathbb{E}_2 = (\mathcal{N}_{pf}, \eta_2)$ are $\mathcal{R}$-equivalent, written $\mathbb{E}_1 \, \mathcal{R} \, \mathbb{E}_2$, if $\eta_1(C) = \eta_2(C)$ for each equivalence class C in $\mathcal{N}_{pf}/\mathcal{R}$.*

Below follows our definition of weak bisimulation.

Definition 4. *Given a PMF pf, an equivalence relation $\mathcal{S} \subseteq \mathcal{N}_{pf} \times \mathcal{N}_{pf}$ is a weak bisimulation under pf if $E \, \mathcal{S} \, F$ implies $l_E \asymp^{pf} l_F$ for any $l \in L$ and for each $\sigma^{pf} \in \Sigma^{pf}$ whenever $E \bullet \sigma^{pf} \xrightarrow{\alpha} \mathbb{E}$ then:*

1. *if $\alpha = y(x)@l$ then there exists $F \bullet \sigma^{pf} \overset{\alpha}{\Longrightarrow} \mathbb{F}$ s.t. for each $z \in N$, $\mathbb{E}\{z/x\} \, \mathcal{S} \, \mathbb{F}\{z/x\}$.*
2. *if $\alpha = (x, \mathbb{L}) \triangleleft l$ then there exists $F \bullet \sigma^{pf} \overset{(x,\mathbb{L})\triangleleft m}{\Longrightarrow} \mathbb{F}$ s.t. for each $z \in N$, $\mathbb{E}\{z/x\} \, \mathcal{S} \, \mathbb{F}\{z/x\}$ and $l_E \asymp^{pf} m_F$.*
3. *if $\alpha = \langle x, \mathbb{L}\rangle@l$ then there exists $F \bullet \sigma^{pf} \overset{\langle x,\mathbb{L}\rangle@m}{\Longrightarrow} \mathbb{F}$ s.t. $\mathbb{E} \, \mathcal{S} \, \mathbb{F}$ and $l_E \asymp^{pf} m_F$.*
4. *otherwise there exists $F \bullet \sigma^{pf} \overset{\alpha}{\Longrightarrow} \mathbb{F}$ and $\mathbb{E} \, \mathcal{S} \, \mathbb{F}$.*

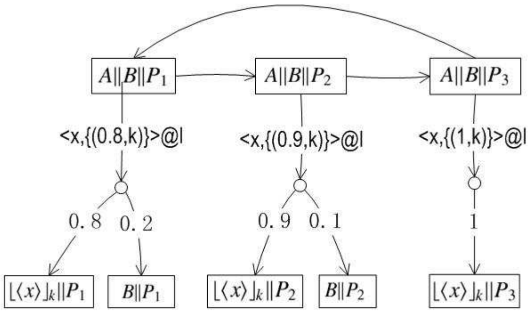
$A\|B\|P_1$
$A\|B\|P_2$
$A\|B\|P_3$
<x,{(0.8,k)}>@l
<x,{(0.9,k)}>@l
<x,{(1,k)}>@l
0.8
0.2
0.9
0.1
1
$\lfloor\langle x\rangle\rfloor_k\|P_1$
$B\|P_1$
$\lfloor\langle x\rangle\rfloor_k\|P_2$
$B\|P_2$
$\lfloor\langle x\rangle\rfloor_k\|P_3$

Fig. 7. Network derivations.

Two networks E and F are weak bisimular under a given PMF pf, written $E \approx_{pf} F$, if $E\ \mathcal{S}\ F$ for some weak bisimulation $\mathcal{S}$ under pf.

Clauses 1 and 4 in Definition 4 are standard. Clause 2 requires that if nodes at locations $l(\mathbb{L})$ in network E can receive a message from location l with specific probabilities, then nodes at locations $l(\mathbb{L})$ in F must be able to receive the same message from some location m with the same probabilities which is mobility equivalent to l. Clause 3 means that if E can broadcast a message from l with receivers at locations $l(\mathbb{L})$, then F can also broadcast the same message from some location m to $l(\mathbb{L})$ with the same probabilities. In addition, l and m are required to be mobility equivalent. Notice that none of the resulting distributions in a bisimulation contains unknown probabilities because of σ^{pf}, and observe that all possible σ^{pf} are taken into account and hence all possible values of otherwise unknown connection information are considered.

Theorem 1. *$\approx_{pf}$ is a congruence.*

To illustrate our weak bisimulation we give the following example.

Example 3. Suppose two nodes $A = \lfloor\langle x\rangle\rfloor_l$, $B = \lfloor(y).\langle y\rangle\rfloor_k$ and connection information: $P_1 = \{\{0.8, k\} \longmapsto l\}$, $P_2 = \{\{0.9, k\} \longmapsto l\}$, $P_3 = \{\{1, k\} \longmapsto l\}$. Let the mobility of $\rho_{k\longmapsto l}$ be given by pf in Fig. 6. It is then not hard to see that $A\|B\|P_1 \approx_{pf} A\|B\|P_2 \approx_{pf} A\|B\|P_3$. The derivation is shown in Fig. 7 where we only show the essential transitions and omit others. Observe that in each of the three networks B can always receive the message from A with probability 0.8, 0.9, or 1.

5 Characterization

In this section we will examine the relation between our calculus and a variant of PCTL* [1] which is a standard modal logic used for expressing properties of probabilistic systems. We use $\mathbb{E}(E)$ to denote the probability of the equivalence class which contains E in a distribution $\mathbb{E}$ and define the (weak) infinite *paths* of a network E under a given pf

by: [1]

$$\Omega_E = \{E_0\alpha_0E_1\ldots \mid \exists\sigma^{pf}.E_0 = E \bullet \sigma^{pf} \wedge \forall i \geq 0\ \exists\mathbb{E}_{i+1}.\ E_i \overset{\alpha_i}{\Longrightarrow} \mathbb{E}_{i+1} \wedge \mathbb{E}_{i+1}(E_{i+1}) \neq 0\}$$

For $\omega = E_0\alpha_0E_1\alpha_1... \in \Omega_E$ we denote by $\omega|_i$ the finite path $E_0\alpha_0E_1...\alpha_{i-1}E_i$ in which case we let $\omega|^i = E_i$, and we define $\Omega_E|_i = \{\omega|_i \mid \omega \in \Omega_E\}$. Notice that as usual due to non-determinism we cannot define a probability measure on Ω_E. To resolve this we, like in e.g.[9, 10], define a *policy*. An *i-level policy* for Ω_E is a partial function

$$\pi_i : \Omega_E|_i \times \mathcal{A} \hookrightarrow ND$$

defined by $\pi_i(\omega|_i, \alpha) = \mathbb{E}$ if there exists $\omega|^i \overset{\alpha}{\Longrightarrow} \mathbb{E}$. A policy π for Ω_E is a pair consisting of a tuple of i-level policies one for each $i \geq 0$ and $\sigma^{pf} \in \Sigma^{pf}$. It defines a subset of Ω_E denoted by Ω^{π}_E such that

$$\Omega^{\pi}_E = \{\omega \in \Omega_{E\bullet\sigma^{pf}} \mid \forall i \geq 0\ \exists\mathbb{E}, \alpha, E.\ \pi_i(\omega|_i, \alpha) = \mathbb{E} \wedge \mathbb{E}(E) \neq 0 \wedge \omega|_{i+1} = \omega|_i\alpha E\}$$

where $\pi = ((\pi_0, \pi_1, \ldots), \sigma^{pf})$. The probability of a path $E_0\alpha_0E_1\alpha_1\ldots \in \Omega^{\pi}_E$ is defined by $\rho_0 \times \rho_1 \times \ldots$ where for all i, $\pi_i(E_0\alpha_0E_1\alpha_1\ldots E_i, \alpha_i) = \mathbb{E}$ for some $\mathbb{E}$ and $\rho_i = \mathbb{E}(E_{i+1})$.

Let $\mathcal{B}^{\pi}_E$ be the smallest algebra of subsets of Ω^{π}_E that contains all the *basic cylinder sets* $\{\omega \in \Omega^{\pi}_E \mid \omega|^0 = E_0 \wedge ... \wedge \omega|^i = E_i\}$ for all $i \geq 0$ that is closed under complement and countable unions. [2] The measure on paths of Ω^{π}_E, written as $\mu_{\pi,E}$, gives a unique measure on $\mathcal{B}^{\pi}_E$.

Below we give the syntax and the semantics for our logic.

Syntax. There are two kinds of formulas: state formulas *Stat* ranged over by ϕ, ϕ' and sequence formulas *Seq* ranged over by ψ, ψ'. The grammar is as follows:

$$\phi ::= \top \mid a \mid \neg\phi \mid \phi \wedge \phi' \mid \exists\psi \mid P_{\bowtie q}\psi$$

$$\psi ::= \alpha \mid \phi \mid \neg\psi \mid \psi \wedge \psi' \mid \bigcirc\psi \mid \psi\mathcal{U}\psi'$$

In the above, $\bowtie$ stands for one of $=, \leq, \geq, <, >$, q is a rational in [0,1] and $\alpha \in \mathcal{A}$. $a \in \mathsf{AP}$ where AP is the set of atomic propositions. Here we omit the details of AP and only assume that weak bisimular networks satisfy the same atomic propositions. These atomic propositions should also cover the connectivity of networks and be able to distinguish networks with non-equivalent connectivity. For example, if we have a network E such that $\rho_{l\longmapsto k}(E) = 0.8$ then we could say that E satisfy proposition $\rho_{l\longmapsto k} = 0.8$.

Semantics. For a formula $\phi \in Stat$, we indicate by $E \models_{pf} \phi$ its satisfaction on network E, and for $\psi \in Seq$ its satisfaction on the path ω is denoted by $\omega \models_{pf} \psi$ under a given PMF pf. The semantics of the logical connectives are defined in the usual way; the

[1] Notice that no path from a network E needs to be finite.

[2] By standard measure theory this algebra is the *Borel σ-algebra* and all its elements are the measurable sets of paths.

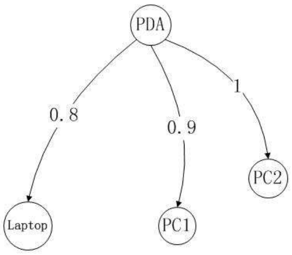

Fig. 8. A home network.

semantics of the remaining operators is defined below:

$$\begin{aligned}
\omega &\models_{pf} \alpha \text{ iff } \omega = E_0\alpha_0E_1\ldots \wedge \alpha_0 =_{pf} \alpha\\
\omega &\models_{pf} \bigcirc\psi \text{ iff } \omega = E_0\alpha_0E_1\ldots \wedge E_1\alpha_1\ldots \models_{pf} \psi\\
\omega &\models_{pf} \psi\mathcal{U}\psi' \text{ iff } \omega = E_0\alpha_0E_1\ldots \wedge \exists i \geq 0.(E_i\alpha_i\ldots \models_{pf} \psi' \wedge \forall 0 \leq j < i.E_j\alpha_j\ldots \models_{pf} \psi)\\
E &\models_{pf} \exists\psi \text{ iff } \exists\pi, \omega \in \Omega_E^\pi.\ \omega \models_{pf} \psi\\
E &\models_{pf} P_{\bowtie q}\psi \text{ iff } \forall\pi.\ \mu_{\pi,E}(\{\omega \in \Omega_E^\pi \mid \omega \models_{pf} \psi\}) \bowtie q
\end{aligned}$$

In the above $\langle x, \mathbb{L}\rangle@l =_{pf} \langle x, \mathbb{L}\rangle@m$ iff $l \asymp^{pf} m$, it is similar for receptions. Intuitively, $E \models_{pf} P_{\bowtie q}\psi$ denotes the probability for the path from E satisfying ψ is $\bowtie q$. With this we can express many kinds of properties such as greatest and lowest bounds and intervals. For example, $P_{\geq q}\psi$ can be used to denote that the lowest bound is q while $P_{\geq q_1}\psi \wedge P_{<q_2}\psi$ guarantees that the probability is in interval $[q_1, q_2)$ with $q_1 < q_2$.

The following are the main results of this section which show the soundness and completeness of weak bisimulation with respect to PCTL*.

Theorem 2. *If $E \approx_{pf} F$ then for all $\phi \in Stat$, $E \models_{pf} \phi$ iff $F \models_{pf} \phi$.*

Theorem 3. *If for all $\phi \in Stat$, $E \models_{pf} \phi$ iff $F \models_{pf} \phi$, then $E \approx_{pf} F$.*

6 The Zeroconf Protocol

The Zeroconf protocol is designed for self-configuring home local networks. For example, Fig. 8 gives a typical home local network which contains four nodes: PC1, PC2, Laptop, and PDA. The arrows indicate that PC1, PC2, and Laptop can receive messages from PDA with probability 0.9, 1, and 0.8 respectively. Here we assume that all other connections have probability 1.

In order to ensure mutual communication, each node must have an unique IP address, so when a new node joins a network it must be assigned an unused IP address. The Zeroconf protocol solves this in the following way:

1. The new node selects an IP address out of all available IP addresses randomly;
2. It broadcasts a message to other nodes to probe if the selected IP address is in use or not;

Table 3. The Zeroconf protocol.

$$
\begin{aligned}
&\mathit{oldnode}_{ip} = !((x).(\mathit{if}\ x = ip\ \mathit{then}\ \langle \mathit{error} \rangle\ \mathit{else}\ 0))\\
&\mathit{newnode}_i^p = \langle p \rangle.\mathit{waitawk}_i^p\\
&\mathit{newnode}_0^p = \langle \mathit{success} \rangle\\
&\mathit{waitawk}_i^p = (x).(\mathit{if}\ x = \mathit{error}\ \mathit{then}\ \mathit{newnode}\ \mathit{else}\ \mathit{waitawk}_i^p) + \mathit{newnode}_{i-1}^p\\
&\mathit{newnode} = \nu y(y(p).\langle p \rangle.\mathit{waitawk}_{pn}^p \| \textstyle\prod_{ip \in IP} \bar{y}\langle ip \rangle)
\end{aligned}
$$

3. If the new node receives a message indicating the IP address is already taken, then it returns to step 1 and restarts the process;
4. Due to unreliable connections, messages can be lost with a certain probability. To increase the reliability of the protocol, the new node is required to send several probes for the same IP address;
5. If no error message has been received after these probes, the selected IP address will be used by the new node.

Note that after running the protocol it is indeed possible for a new node to use an IP address that is already used by another node. This is called address collision and is highly undesirable.

In the following, we model and analyse the Zeroconf protocol, the model of the protocol is given in Table 3. [3] We use $\mathit{oldnode}_{ip}$ to denote an existing network node, i.e. a process with IP address ip running at a location; $\mathit{oldnode}_{ip}$ repeatedly receives messages and compare these messages with its own IP address ip. If a message is identical to ip, it will broadcast an error message, *error*, informing the new node that the selected IP address is being used already; $\mathit{newnode}_i^p$ denotes a process which will probe i times before assuming that the selected IP address p is not used by other nodes. It will evolve into process $\mathit{waitawk}_i^p$ after broadcasting a probe. $\mathit{newnode}_0^p$ is a special process which denotes that the protocol succeeded in finding an unused IP address p (although this might not be true with a certain probability); $\mathit{waitawk}_i^p$ waits for the responses from other nodes. If it receives an *error* message because the selected IP address is not valid, it will restart the whole process, otherwise it will recurse and become $\mathit{waitawk}_i^p$ again. The summation here is used to denote timeout from waiting for responses and then start a new round of probing. *newnode* starts the protocol by selecting an IP address from IP randomly, here IP is the set of all available addresses and $\prod$ means parallel composition of processes. In the above, we use pn to denote the maximum number of probes for the same IP address.

The behavior of the network in Fig. 8 can be represented as follows:

$$E = \lfloor \mathit{newnode} \rfloor_k \ \|\ \lfloor \mathit{oldnode}_{ip_1} \rfloor_l \ \|\ \lfloor \mathit{oldnode}_{ip_2} \rfloor_m \ \|\ \lfloor \mathit{oldnode}_{ip_3} \rfloor_n$$

We assume Laptop, PC1, and PC2 are existing nodes which are located at l, m, and n respectively, and PDA at k is a node that wants to join the network; here ip_1, ip_2, and ip_3 are used to denote IP addresses in IP already in use. Concerning mobility we assume a PMF pf such that the mobility rules of $\rho_{k \longmapsto l}$ and $\rho_{k \longmapsto m}$ are given by Fig. 4 and the

[3] Summation is defined by: $P + Q = \nu x(\bar{x}\langle y \rangle \| x(y).P \| x(y).Q)$.

mobility rule of $\rho_{k\longmapsto n}$ is given by Fig. 6, in addition all the other connections are always equal to 1.

In the following, we use $\langle x\rangle @\tilde{l}$ as a shorthand of $\vee_{l\in\tilde{l}}\langle x,\mathbb{L}\rangle @l$ where $\mathbb{L}$ ranges over all the location connection sets. With the PCTL* logic introduced in the above section, we can denote the obvious property that ”if an unused IP address is selected by the new node then the probability of this IP address being allocated to the new node is equal to 1”, formally we have:

$$\phi = P_{=1}(\vee_{ip\in IP\setminus\{ip_1,ip_2,ip_3\}}\langle ip\rangle @k \rightarrow \diamond(\neg\langle error\rangle @\{l,m,n\} \wedge \langle success\rangle @k))$$

letting $\diamond\psi \overset{def}{=} \top\mathcal{U}\psi$. Clearly $E \models \phi$. We may also specify the property: ”if an used IP address is selected by the new node then the probability of address collision is less than q”. Formally we have:

$$\phi_q = P_{\leq q}(\vee_{i\in\{1,2,3\}}\langle ip_i\rangle @k\mathcal{U} \vee_{i\in\{1,2,3\}} \langle ip_i\rangle @k \rightarrow \diamond(\neg\langle error\rangle @\{l,m,n\} \wedge \langle success\rangle @k))$$

Assuming the maximum number of probes pn to be 3 it turns out that $E \not\models \phi_{0.001}$ while $E \models \phi_{0.008}$. Intuitively, if the new node selects an used IP address such as ip_1, then among all policies to consider there exists a worst case policy under which $oldnode_{ip_1}$ may fail to receive the probe from the new node for three times with probability $(1-0.8)^3 = 0.008$.

In order to illustrate analysis through the use of weak bisimulation we may define

$$F \equiv \lfloor newnode\rfloor_k \parallel \lfloor oldnode_{ip_1}\rfloor_l \parallel \lfloor oldnode_{ip_3}\rfloor_m \parallel \lfloor oldnode_{ip_2}\rfloor_n$$

i.e. compared to E in the network F the two old nodes PC1 and PC2 have swapped their locations m and n. Further let

$$E' \equiv \{\{(k,0.8)\} \longmapsto l\}||\{\{(k,1)\} \longmapsto m\}||\{\{(k,0.9)\} \longmapsto n\}$$

and let

$$F' \equiv \{\{(k,1)\} \longmapsto l\}||\{\{(k,0.9)\} \longmapsto m\}||\{\{(k,0.8)\} \longmapsto n\}$$

then because $m_{E'} \asymp^{pf} n_{F'}$ we infer

$$E||E' \approx_{pf} F||F'$$

Intuitively, by the given pf locations m and n are mobility equivalent and furthermore they can always receive messages from other locations with the same probability. If the new node selecting an used IP address such as ip_2 broadcasts a probe, then the node at location m in E can receive it with probability 1 and then broadcast an *error* message. The node at location n in F can simulate this by performing the same actions in addition with some mobility transitions. In both E and F, the *newnode* can receive the *error* message with the same probability. A similar argument holds for other transitions.

7 Conclusion and Future Works

The main contribution of this paper is the development of a probabilistic broadcast calculus for mobile and wireless networks with unreliable connections in that broadcasted messages can be lost with a certain probability. Moreover, due to a *probabilistic mobility function* connections between locations may change with certain probabilities.

We have given a labeled transition system semantics for our calculus on which we define a probabilistic weak bisimulation equivalence parameterized by a probabilistic mobility function. Two bisimular networks need not have the same connectivity information and also they may broadcast the same messages from different locations. To the best of our knowledge, the integration of bisimulation, probabilistic loss of broadcasted messages, and probabilistic mobility functions is a novel contribution. Also, we have characterized our weak bisimulation by a variant of PCTL*.

A number of further developments are possible. One of them is that we could enrich the calculus by adding probability at the process level. This would allows to model e.g. randomized backoff protocols for wireless systems. Also the Zeroconf protocol example could be improved by having a randomized timeout instead of just using nondeterminism. Since time is important for wireless network, another extension is to consider a timed version of our calculus like in [11].

References

1. Desharnais, J., Gupta, V., Jagadeesan, R., Panangaden, P.: Weak Bisimulation is Sound and Complete for PCTL*. In: Brim, L., Jancar, P., Kretínský, M., Kucera, A. (eds.) CONCUR 2002. LNCS, vol. 2421, pp. 355–370. Springer, Heidelberg (2002)
2. Baier, C., Katoen, J.P.: Principles of Model Checking. MIT Press (2008)
3. Nanz, S., Hankin, C.: A Framework for Security Analysis of Mobile Wireless Networks. Theoretical Computer Science. 367(1-2), 203–227 (2006)
4. Singh, A., Ramakrishnan, C.R, Smolka, S.A.: A Process Calculus for Mobile Ad Hoc Networks. In Olso, D. Lea, G. Zavattaro (eds.) COORDINATION 2008. LNCS, vol. 5052, pp. 296–314. Springer, Heidelberg (2008)
5. Merro, M.:An Observational Theory for Mobile Ad-hoc Networks. Electronic Notes in Theoretical Computer Scienc, vol. 173, pp. 275–293. Elsevier (2007)
6. Ghassemi, F., Fokkink, W., Movaghar, A.: Restricted Broadcast Process Theory. In: Proceedings of 6th Conference on Software Engineering and Formal Methods (SEFM'08), pp. 345–354. IEEE Press (2008)
7. Godskesen, J.C.: A Calculus for Mobile Ad-hoc Networks. In Paphos, Murphy, A.L., Vitek, J. (eds.) COORDINATION'07. LNCS, vol. 4467, pp. 132–150. Springer, Heidelberg (2007)
8. Godskesen, J.C.: A Calculus for Mobile Ad-hoc Networks with Static Location Binding. In: 15th International Workshop on Expressiveness in Concurrency (2008)
9. Segala, R., Lynch, N.: Probabilistic Simulations for Probabilistic Processes. In Uppsala, Jonsson, B., Parrow, J. (eds.) CONCUR'94. LNCS, vol. 836, pp. 481–496. Springer, Heidelberg (1994)
10. Philippou, A., Lee, I., Sokolsky, O.: Weak Bisimulation for Probabilistic Systems. In PA, Palamidessi, C. (eds.) CONCUR'00. LNCS, vol. 1877, pp. 334–349. Springer, Heidelberg (2000)
11. Merro, M., Sibilio, E.: A Timed Calculus for Wireless Systems. In: 3rd International Conference on Fundamentals of Software Engineering (FSEN'09) (2009)