マルチメディア通信と分散処理　94－20
分散システム/インターネット運用技術　14－20
（１９９９．７．１６）

有限状態モデルに基づくモバイルシステムの仕様化

板橋 吾一，高橋 薫，加藤 靖
仙台電波工業高等専門学校

並行システムにおいては，エンティティ(システム構成要素) 間の結びつきによって相互作用が行なわれ，結びつきはシステム全体の構造を決定する．この並行システムの１つとしてモバイルシステムが挙げられる．モバイルシステムにおいて，エンティティはシステム内を自由に移動し，結びつきは静的なだけでなく動的にも確立・切断されている．このようなシステムの挙動は一般に複雑であり，システムの設計も難しくなる．本稿では，まずエンティティの存在する場を導入し相互作用を局所的なものとして扱う．そしてエンティティを通信型有限状態機械の概念でモデル化し，エンティティの移動と結びつきの動的変化を陽に考慮することによって，モバイルシステムのモデル化及び形式的仕様化法を提案する．

Specification of a Mobile System based on Finite State Model

Goichi Itabashi, Kaoru Takahashi and Yasushi Kato
Sendai National College of Technology

In a concurrent system, interactions take place via associations among entities (i.e. system components), and the associations determine the structure of the system. A mobile system is a typical one of the concurrent systems. In a mobile system, entities can arbitrarily migrate over the system, and the association among entities can be established and disconnected dynamically as well as statically. The behavior of such a system is generally complicated, and the designing of the system becomes difficult. In this paper, we propose a modeling and formal specification method for a mobile system. In this method, the concept of a field where entities exist is introduced, and interactions among the entities are dealt with locally. We model an entity as a communicating finite state machine, and consider migration of an entity and dynamic change of associations among entities.

1　まえがき

分散並行システムにおいて，システム構成要素(エンティティ) 間には何らかの結びつきが存在し，エンティティ間の結びつきは並行システム全体の構造を決定する．このような分散並行システムの一つとして移動通信が考えられる [1]．移動通信では，セルラー方式やPHSに見られるように，移動局と基地局との交信可能な領域を狭くし，その分だけ基地局を多く配置して無線周波数の再利用を行っている．移動通信では，移動局，つまりエンティティがシステム内を自由に移動し，エンティティ間の結びつきを静的なだけではなく動的にも確立・切断することによって全体の処理が実行される．その結果システム全体の構造は動的に変化し，システムの設計は難しくなる．

上記のようなモバイルシステムを設計するためには，システムを曖昧なく厳密に仕様化する事が望ましい．これにより仕様段階でのシステムの解析が可能となり，システム設計の高信頼化が達成できる．

本稿では，エンティティを通信型有限状態機械(CFSM: Communicating Finite State Machine)[3, 4, 5, 6] の概念を用いてモデル化する．そして，エンティティの移動に伴うエンティティ間の結びつきの動的な変化を考慮することによって，モバイルシステムのより強力なモデル化および形式的仕様化の方法を提案する．モバイルシステムを有限状態機械の集合体とし，エンティティが移動する空間を“場”として考える．結びつきの動的変化は結びつきをチャネルとして表現し，いくつかの有限状態機械がチャネルによる動的な確立・切断を行い，チャネル名を有限状態機械間で受け渡すことによって表現する．またチャネルを介した相互作用は，チャネルを確立した有限状態機械間の同期通信として表

現する．相互作用は局所的なものとして表現する．

以下では，まず有限状態機械のロケーションとチャネルを導入する．次に，有限状態機械の概念に基づいてモバイルシステムのモデル化を考え，その挙動をシステム全体の状態遷移の観点から形式化する．そして，本モデルの適用例を簡単な記述例を通して説明する．最後に，まとめと課題を示す．

2 場

本節では有限状態機械の存在位置を示すロケーションと結びつきを表すチャネルを導入する．次に，相互作用をいくつかのロケーション内に制限する場 [2] をロケーションとチャネルから定義する．これにより有限状態機械間の局所的な相互作用を表現する．

有限状態機械が存在しうるロケーションの有限集合を L とする．有限状態機械はロケーションの上を自由に移動可能であると仮定する．チャネルは有限状態機械間及び環境と有限状態機械との結びつきを表す抽象概念である．環境はモデル化しないシステムの外界を表すと考える．環境と有限状態機械の間には暗黙のチャネルがあると考える．これを環境チャネルと呼び $\mathbf{c_e}$ で表す．有限状態機械間のチャネルの集合は $\mathcal{C}_f$ で表す(1)．

本稿では，有限状態機械間の相互作用はある範囲内に制限され，この相互作用可能な範囲はチャネルによって異なると考える．これを次のように表現する．

定義 1. 有限状態機械の場 F を次のように定義する．

$$F = \{(c_i,\ COM(c_i)) \mid 1 \leq i \leq m\}$$
$$COM(c_i) \subseteq \mathcal{P}(L)$$

□

$c \in \mathcal{C}_f$, $P \subseteq L$ のとき，$P \in COM(c)$ であることは，P に属するロケーションに存在するいくつかの有限状態機械は c で相互作用可能であることを表し，逆に P に属していないロケーションに存在する有限状態機械は c で相互作用することはできないことを表す．あるロケーション l にチャネル c を持ついくつかの有限状態機械が存在している時，$l \in P$ かつ $P \in COM(c)$ なるロケーションの集合 P が存在しなければ，そのいくつかの有限状態機械は c で相互作用することはできない．また，$P, P' \in COM(c)$ $(P \neq P')$ について $P \cap P' = \phi$ でなければならない．以下に場の例を示す．

例

$L = \{1,\ 2,\ 3,\ 4\}$
$\mathcal{C}_f = \{c_1,\ c_2\}$
$F = \{(c_1,\ COM(c_1)),\ (c_2,\ COM(c_2))\}$
$COM(c_1) = \{\{1,\ 2,\ 3\}\}$
$COM(c_2) = \{\{1,\ 2\},\ \{3,\ 4\}\}$

(1)便宜上，$|\mathcal{C}_f| = m$ と固定し，$\mathcal{C}_f$ の各要素を $c_1, \cdots, c_i, \cdots, c_m$ で表す．

この場の上にチャネル c_1，c_2 を持つ $CFSM_1$，$CFSM_2$，$CFSM_3$ を配置したのが図 1 である．この例では，ロケーション 1, 2, 3 にいる $CFSM_1$, $CFSM_2$, $CFSM_3$ はチャネル c_1 で互いに相互作用可能である．また，$CFSM_1$ と $CFSM_2$ はチャネル c_2 で相互作用可能であるが $CFSM_3$ は $CFSM_1$, $CFSM_2$ と相互作用することができない．

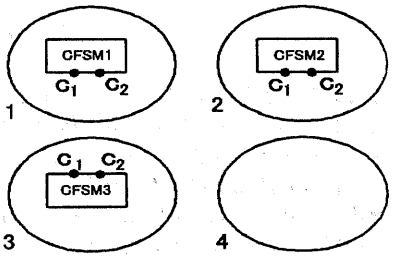

図 1: 場の例

3 システムのモデル化

モバイルシステムを，チャネルによる相互作用を行ういくつかの有限状態機械の集まりとしてモデル化する．

定義 2. モバイルシステム Sys を

$$Sys = \langle (CFSM_1, \cdots, CFSM_k, \cdots, CFSM_n), \mathcal{C} \rangle$$

で定義する．ここで $\mathcal{C}$ $(\mathcal{C} = \mathcal{C}_f \cup \{\mathbf{c_e}\})$ は Sys のチャネルの有限集合を表す．$CFSM_k (1 \leq k \leq n)$ は通信型有限状態機械であり次のように定義する．

$CFSM_k = \langle Q_k, C_k, E_k, \delta_k, q_{k0} \rangle$

Q_k : $CFSM_k$ の状態の有限集合

C_k : $CFSM_k$ が持ちうるチャネルの集合 $(C_k \subseteq \mathcal{C})$

E_k : $CFSM_k$ のイベントの集合

$E_k \subseteq (C_k \times (\Sigma_k \cup \Sigma_k^2 \cup \cdots \cup \Sigma_k^t))$
$\cup (C_k \times A) \cup (\{move\} \times L) \cup \{\varepsilon\}$

$\Sigma_k = I_k \cup O_k$

I_k : $CFSM_k$ の入力の集合

O_k : $CFSM_k$ の出力の集合

A: $CFSM_k$ の制御の集合

$A = \{connect,\ disconnect\}$

$connect$: チャネル確立

disconnect: チャネル切断

move: ロケーションの移動

L: ロケーションの集合

ε: 内部イベント

δ_k: $CFSM_k$ の状態遷移関数

$\delta_k : E_k \times Q_k \longrightarrow Q_k$

q_{k0} : $CFSM_k$ の初期状態 $q_{k0} \in Q_k$

□

$(c, \alpha_1, \cdots, \alpha_h) \in E_k (1 \leq h \leq t)$ は, $CFSM_k$ の入出力列 $\alpha_1, \cdots, \alpha_h$ がチャネル $c \in C_k$ を対象として生起しうることを表す. $(c, a) \in E_k (a \in A)$ は, 制御 a がチャネル $c \in C_k$ を対象として生起しうることを表す. $(move, l) \in E_k$ は $CFSM_k$ のロケーション l への移動を表し, '$\hookrightarrow$' の記号で表す. $\varepsilon \in E_k$ は内部イベントであり, 他の有限状態機械と同期をとらずに有限状態機械内部で勝手に生起できる性質を持つ. $CFSM_k$ における状態遷移はこれらのイベントの生起により可能となる.

制御には *connect*(チャネルの確立) と *disconnect*(チャネルの切断) があり, 入力または出力は環境も含めて $n (n \geq 2)$ 個の有限状態機械間及び環境と有限状態機械との間にチャネルが確立して始めて可能になる. すなわちチャネルが確立されている時のみ互いの入出力が可能となる. 但し, 環境チャネルは暗黙に確立されていると仮定する. 有限状態機械間及び環境で入出力されるオブジェクトにはメッセージとチャネルの 2 つの型がある. メッセージはチャネル以外の意味を持つ情報を表している. 但し, $\mathbf{c_e}$ の入出力は行わないものとする.

定義 3. 個々の有限状態機械に対する記法・記号を以下のように定義する.

(1) $\#c$	チャネル c での接続
(2) $/c$	チャネル c での切断
(3) $?x$	メッセージ x の入力
(4) $??y$	チャネル y の入力
(5) $!m$	メッセージ m の出力
(6) $!!c$	チャネル c の出力
(7) $c\alpha_1 \cdots \alpha_i \cdots \alpha_h$	チャネル c での入出力列 $\alpha_1 \cdots \alpha_h$ ただし, α_i $(1 \leq i \leq h)$ は上の (3) ~ (6) のいずれかである.
(8) $\hookrightarrow l$	ロケーション l への移動
(9) $q \xrightarrow{e} q'$	状態 q から状態 q' へのイベント $e \in E_k$ による遷移

□

4 システムの挙動

本節では, システム Sys 全体の挙動を次の考え方で特性化する. まず, 個々の有限状態機械の状態, 個々の有限状態機械が存在しているロケーション, そして C のチャネルの状態で表現するシステム状態を導入し, システム Sys の挙動をそのようなシステム状態の遷移の系列として定義する. このシステム状態遷移系列は一つのグラフ構造を形成し, このグラフをシステム状態グラフと呼ぶ. システム状態グラフは Sys の挙動全体を表現する.

定義 4. モバイルシステムのシステム状態 s を以下のように定義する :

$$s = \langle (q_1, \cdots, q_k, \cdots, q_n), (l_1, \cdots, l_k, \cdots, l_n), (sc_1, \cdots, sc_i, \cdots, sc_m, sc_e) \rangle$$

ここで, q_k $(1 \leq k \leq n)$ は $CFSM_k$ の状態である. $l_k \in L$ $(1 \leq k \leq n)$ は $CFSM_k$ の存在しているロケーションを示している. そして, sc_i $(1 \leq i \leq m)$ 及び sc_e はチャネル c_i, $\mathbf{c_e} \in C$ で形成されたグループ g_p の集合 $\{g_p\}$ であり, 具体的には環境も含めた有限状態機械のベキ集合である(2).

□

定義 5. システム状態グラフ G は次の 4 項組である :

$$G = \langle\ S, E, \delta, s_0\ \rangle$$

ここで, S はシステム状態の集合, E はイベントの集合, δ $(\delta : S \times E \to S)$ はシステム状態の遷移関数, s_0 は初期システム状態である. なお, E は, 有限状態機械間のチャネル接続 (グループの形成), グループ内での入出力, そしてチャネルの切断 (グループの解消) から成る.

□

定義 6. システム状態に対する記法・記号を次のように定義する.

$\#c\{a, b, \cdots\}$
チャネル c での $CFSM_a, CFSM_b, \cdots$ による チャネル確立 (グループの形成イベント)

$/c\{a, b, \cdots\}$
チャネル c での $CFSM_a, CFSM_b, \cdots$ による チャネル切断 (グループの解消イベント)

$c\{a, b, \cdots\}(u_1, u_2, \cdots)$
チャネル c での $CFSM_a, CFSM_b, \cdots$ による 入出力オブジェクト $(u_1, u_2, \cdots)$ の入出力 (グループ内入出力イベント)

(2)環境は *env* で表す.

$\varepsilon\{a\}$
$CFSM_a$ の内部イベントの生起 □

メッセージやチャネルの入力は有限状態機械における変数[3]への代入によって表し，以下のように定義する．なお値の代入されていない変数は変数名をそのまま値として扱う．有限状態機械内において，変数はすべて異なるものと仮定する．すなわち，変数名は有限状態機械中でグローバルであり，ローカル変数の概念はない．

定義 7. 有限状態機械 $CFSM_k$ における変数 u に値 v を代入することを以下の記法で定義する:
$[u := v]CFSM_k$

□

定義 8. モバイルシステム $Sys = \langle (CFSM_1, \cdots, CFSM_k, \cdots, CFSM_n), C \rangle$, 場 $F = \{(c_i, COM(c_i)) \mid 1 \leq i \leq m\}$, そして各 $CFSM_k$ の初期ロケーション l_{k0} が与えられたとき，これに対応するシステム状態グラフ

$$G = \langle S, E, \delta, s_0 \rangle$$

を以下の規則の適用により推論される最小のものとして定義する：

1. 初期システム状態
   $s_0 = \langle (q_{10}, \cdots, q_{k0}, \cdots, q_{n0}), (l_{10}, \cdots, l_{k0}, \cdots, l_{n0}), (sc_1, \cdots, sc_i, \cdots, sc_m, sc_e) \rangle \in S$,
   ここで, $sc_i = \phi$ $(1 \leq i \leq m)$,
   $sc_e = \{\{CFSM_1, env\}, \cdots, \{CFSM_n, env\}\}$.

2. チャネル確立 (グループ形成) [4]
   $s = \langle (\cdots, q_a, \cdots, q_z, \cdots), (\cdots, l_a, \cdots, l_z, \cdots), (\cdots, sc_i, \cdots) \rangle \in S$,
   $q_a \xrightarrow{\#c_i} q'_a, \cdots, q_z \xrightarrow{\#c_i} q'_z$,
   $\{l_a, \cdots, l_z, \cdots\} \in COM(c_i)$,
   $(c_i, COM(c_i)) \in F$,
   $\{CFSM_a, \cdots, CFSM_z\} \notin sc_i$
   ならば
   $s' = \langle (\cdots, q'_a, \cdots, q'_z, \cdots), (\cdots, l_a, \cdots, l_z, \cdots), (\cdots, sc'_i, \cdots) \rangle \in S$,
   $sc'_i = sc_i \cup \{\{CFSM_a, \cdots, CFSM_z\}\}$,
   $s \xrightarrow{\#c_i\{a,\cdots,z\}} s'$.

3. 入出力オブジェクトの入出力 (グループ内入出力イベント)
   ◇ c_i における入出力オブジェクトの入出力[5]
   $s = \langle (\cdots, q_a, \cdots, q_z, \cdots), (\cdots, l_a, \cdots, l_z, \cdots), (\cdots, sc_i, \cdots) \rangle \in S$,
   $q_a \xrightarrow{c_i\alpha_{a1}\cdots\alpha_{aj}\cdots\alpha_{ah}} q'_a, \cdots, q_z \xrightarrow{c_i\alpha_{z1}\cdots\alpha_{zj}\cdots\alpha_{zh}} q'_z$,
   $\{l_a, \cdots, l_z, \cdots\} \in COM(c_i)$,
   $(c_i, COM(c_i)) \in F$,
   $\{CFSM_a, \cdots, CFSM_z\} \in sc_i$,
   但し, 各イベント $\alpha_{aj}, \cdots, \alpha_{zj}$ $(1 \leq j \leq h)$ は次の条件のどちらかを満たす:
   (1) ある r $(r \in \{a, \cdots, z\})$ について, $\alpha_{rj} = !m$ のとき, すべての t $(t \in \{a, \cdots, z\} - \{r\})$ について $\alpha_{tj} = ?x_t$.
   (2) ある r $(r \in \{a, \cdots, z\})$ について, $\alpha_{rj} = !!c$ のとき, すべての $t(t \in \{a, \cdots, z\} - \{r\})$ について $\alpha_{tj} = ??y_t$.
   ならば
   $s' = \langle (\cdots, q'_a, \cdots, q'_z, \cdots), (\cdots, l_a, \cdots, l_z, \cdots), (\cdots, sc_i, \cdots) \rangle \in S$,
   $\alpha_{aj}, \cdots, \alpha_{zj}$ が上の条件 (1), (2) のどちらを満たすかにより以下とする:
   (1) のとき, すべての $t(t \in \{a, \cdots, z\} - \{r\})$ について $[x_t := m]CFSM_t$.
   (2) のとき, すべての $t(t \in \{a, \cdots, z\} - \{r\})$ について $[y_t := c]CFSM_t$.
   $s \xrightarrow{c_i\{a,\cdots,z\}\theta} s'$.
   但し, $\theta = (val_c(\alpha_{a1}, \cdots, \alpha_{z1}), \cdots, val_c(\alpha_{ah}, \cdots, \alpha_{zh}))$
   ここで, $val_c(\alpha, \beta, \cdots)$ はイベント $\alpha, \beta, \cdots$ から出力イベントの値 (メッセージまたはチャネル) を取り出すことを表す.

◇ $\mathbf{c_e}$ における入出力オブジェクトの入出力
$s = \langle (\cdots, q_k, \cdots), (\cdots), (\cdots) \rangle \in S$,
$q_k \xrightarrow{\mathbf{c_e}\alpha_1\cdots\alpha_j\cdots\alpha_h} q'_k$
ならば
$s = \langle (\cdots, q'_k, \cdots), (\cdots), (\cdots) \rangle \in S$,
環境の持つメッセージの集合とチャネルの集合をそれぞれ MSG, CH とし,
各 $\alpha_j (1 \leq j \leq h)$ に対して以下とする:
(1)$\alpha_j = ?x$ のとき,
$[x := msg]CFSM_k$ $(msg \in MSG)$.
(2)$\alpha_j = ??y$ のとき,
$[y := ch]CFSM_k$ $(ch \in CH)$.
$s \xrightarrow{\mathbf{c_e}\{k,env\}\theta} s'$.
但し, $\theta = (val_{\mathbf{e}}(\alpha_1), \cdots, val_{\mathbf{e}}(\alpha_j), \cdots, val_{\mathbf{e}}(\alpha_h))$
ここで, $val_{\mathbf{e}}(\alpha)$ は以下を表す:
(1)$\alpha = ?x$ のとき,
$val_{\mathbf{e}}(\alpha) = msg$ $(msg \in MSG)$
(2)$\alpha = ??y$ のとき,
$val_{\mathbf{e}}(\alpha) = ch$ $(ch \in CH)$
(3)$\alpha = !m$ のとき, $val_{\mathbf{e}}(\alpha) = m$
(4)$\alpha = !!c$ のとき, $val_{\mathbf{e}}(\alpha) = c$.

[3] $?x$ や $??y$ として各有限状態機械内で宣言される.
[4] ここで, チャネル c_i でグループを形成しようとしている有限状態機械を $CFSM_a, \cdots, CFSM_z$ と表す. またそれぞれが存在するロケーションを $l_a, \cdots, l_z$ と表す.
[5] ここで, チャネル c_i でグループを形成している有限状態機械を $CFSM_a, \cdots, CFSM_z$ と表す. またそれぞれが存在するロケーションを $l_a, \cdots, l_z$ と表す.

4. チャネル切断 (グループの解消) [6]

$s = \langle(\cdots, q_a, \cdots, q_z, \cdots),$
$(\cdots, l_a, \cdots, l_z, \cdots), (\cdots, sc_i, \cdots)\rangle \in S,$
$q_a \xrightarrow{/c_i} q'_a, \cdots, q_z \xrightarrow{/c_i} q'_z,$
$\{l_a, \cdots, l_z, \cdots\} \in COM(c_i),$
$(c_i, COM(c_i)) \in F$
$\{CFSM_a, \cdots, CFSM_z\} \in sc_i$
ならば
$s' = \langle(\cdots, q'_a, \cdots, q'_z, \cdots),$
$(\cdots, l_a, \cdots, l_z, \cdots), (\cdots, sc'_i, \cdots)\rangle \in S,$
$sc'_i = sc_i \setminus \{\{CFSM_a, \cdots, CFSM_z\}\},$
$s \xrightarrow{/c_i\{a,\cdots,z\}} s'.$

5. 移動イベント

$s = \langle(\cdots, q_k, \cdots), (\cdots, l_k, \cdots),$
$(\cdots)\rangle \in S,$
$q_k \xrightarrow{\hookrightarrow l'_k} q'_k$
ならば
$s' = \langle(\cdots, q'_k, \cdots), (\cdots, l'_k, \cdots),$
$(\cdots)\rangle \in S,$
$s \xrightarrow{\varepsilon\{k\}} s'.$

6. 内部イベント

$s = \langle(\cdots, q_k, \cdots), (\cdots), (\cdots)\rangle \in S,$
$q_k \xrightarrow{\varepsilon} q'_k$
ならば
$s' = \langle(\cdots; q'_k, \cdots), (\cdots), (\cdots)\rangle \in S,$
$s \xrightarrow{\varepsilon\{k\}} s'.$

□

5 適用例

本節では，具体的な適用例を通して本稿で提案した形式的仕様化法の適用可能性を示す．図 2 は携帯

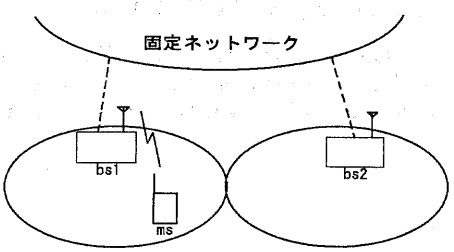

図 2: 移動通信システムの構成図

電話のような移動通信システム [1] の例を表している．システムは 1 つの移動局 (ms) と 2 つの基地局 (bs1, bs2) から構成されているものとする．ms と bs1 および bs2 は無線によって会話の音声信号を入出力し，bs1 および bs2 は固定ネットワーク (制御ネットワーク) と有線で接続され，ms からの音声信号を入出力する．また固定ネットワークはその音声信号のフローを制御し最終的な通話相手へと音声信号を伝達する機能などを持っている．しかし，ここでは簡単化のため固定ネットワークと通話相手は省略し，システムのエンティティを ms, bs1 そして bs2 に限定する．このシステムの場は以下の通りである．

$L = \{1, 2\}, C_f = \{c, f_1, f_2\}$
$F = \{(c, COM(c)), (f_1, COM(f_1)),$
$(f_2, COM(f_2))\}$
$COM(c) = \{\{1\}, \{2\}\}$
$COM(f_1) = \{\{1\}\}$
$COM(f_2) = \{\{2\}\}$

ここでチャネル c は制御信号を入出力する制御チャネルを表し，チャネル f_1, f_2 は音声信号を入出力する通話チャネルを表している．チャネル c はどちらのロケーションでも共通だが独立なチャネルであり，チャネル f_1, f_2 は基地局のあるロケーションごとに個別に割り当てられているチャネルである．また，このシステムで扱われるメッセージには conn, dconn, そして talk がある．conn は ms が bs1/bs2 に対して通話チャネルの接続を要求するメッセージを表し，dconn は ms が bs1/bs2 に通話の終了を通知するメッセージである．そして talk は ms と bs1/bs2 の間で入出力される音声信号である．図 3 は場の上に ms, bs1, bs2 を配置した図である．図 4 は bs1 が ms からの接続要求に対して通話チャネルを割り当てて ms が通話をする手順と，そして ms が通話中にエリア間を移動しても通話を継続するハンドオーバ機能を，本稿で提案した仕様化法を用いて記述したものである．

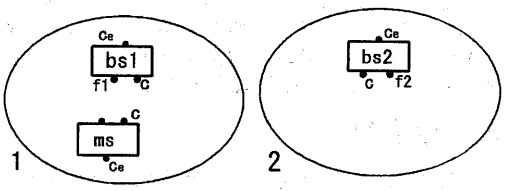

図 3: エンティティの構成図

ms は bs1 と制御チャネル c を確立し，bs1 に対して conn を出力して通話チャネル $f_1(=y)$ を入力する．そして ms は通話チャネル $f_1(=y)$ を確立し，通話チャネルを通して通話 (talk の入出力) を行なう．ここで ms がロケーション 1 から 2 へ移動する時には，移動する前に一度 $f_1(=y)$ と c を切断してから移動する．そしてロケーション 2 に移動した後 bs2 と c でチャネルを確立し conn を出力して通話チャネル $f_2(=y)$ を入力する．そして ms は通話チャネル f_2 を確立して bs2 との通話 (talk の入出力) が可能になり通話が継続できる．本節ではふれないが，以上で説明したシステムの動作は前節で定義した生成規則の適用によるシステム状態グラフで観察することができる．システム状態グラフからは，個々のエンティティの挙動だけでなく，ms と bs1/bs2 の間のネットワーク構造の変化と入出

[6] $CFSM_a, \cdots, CFSM_z$ と $l_a, \cdots, l_z$ は入出力オブジェクトの入出力の場合と同様．

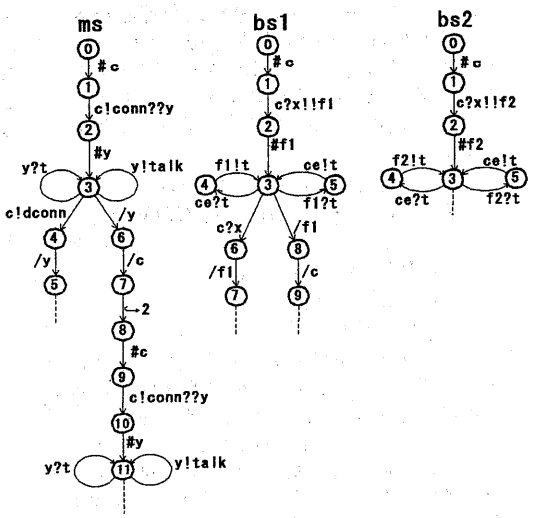

図 4: システム仕様

力されるオブジェクトの受け渡しを観察することができる.

この例から分かるように, 本稿で提案した仕様化法によって, ms と bs1/bs2 間の局所的な相互作用と ms の移動性を表現することができ, さらには ms と bs1/bs2 間の結びつきの動的な確立・切断が明示的に記述可能となる. また, ms の変数 y を ms 自身の移動に伴い f_1 から f_2 へ置き換え, ms は新たに bs2 と通話するというように, エンティティ間の移動に伴うチャネルの組替えが柔軟に表現されている. そして, システム状態グラフではシステム全体の挙動をシステム状態の遷移系列として表すことができ, システム状態グラフからシステムの挙動観察さらには挙動検証も可能となる.

6 むすび

本稿では, エンティティの移動に伴うエンティティ間の結びつきの動的な変化を明示的に表現するために, エンティティが移動する場を導入し, エンティティを通信型有限状態機械の概念でモデル化した. そして, チャネルによるエンティティ間の相互作用を表現することによって, モバイルシステムのモデル化および形式的仕様化の方法を提案した. また, チャネルによって複数のエンティティ間を結びつけ, メッセージさらにはチャネルをグループ内で受け渡しあうことにより, エンティティ間の通信をより柔軟に表現することを可能としている. さらには, システム状態グラフを定義することによって, 仕様からシステム全体の構造の変化やオブジェクトの入出力を観察可能にした. これにより, 仕様レベルでのシステムの挙動解析または挙動検証も可能となる.

今後の課題として次のようなことが考えられる.

- 本稿で提案した仕様化方法に基づく挙動検証支援システムの作成.
- 仕様の複雑性や大規模性に耐えうる有限状態機械の構造化表現 (例えば文献 [6, 7, 8]).

参考文献

[1] 服部武, 花田恵太郎, 古谷之綱, 正木勝, "モーバイルパーソナルインテリジェンス," 共立出版, 1996.

[2] T. Ando, K. Takahashi, Y. Kato and N. Shiratori, "A Concurrent Calculus with Geographical Constraints," IEICE Trans. Fund., Vol.E81-A, No.4, pp.547-555, 1998.

[3] G. J. Holzmann,"Design and Validation of Computer Protocols," Prentice-Hall, 1991.

[4] E. Battiston, F. D. Cindio and G. Mauli, "Modular Algebraic Nets to Specify Concurrent Systems," IEEE Trans. Software Eng., Vol.22, No.10, pp.689-705, 1996.

[5] A. C. Shaw, "Communicating Real-Time State Machines," IEEE Trans. Software Eng., Vol.18, No.9, pp.805-816, 1992.

[6] D. Harel, H. Lachover, A. Naamad, A. Pnueli, M. Politi, R. Sherman, A. S. Trauring and M. Trakhtenbrot, "Statemate: a Working Enviroment for the Development of Complex Reactive System," IEEE Trans. Software Eng., Vol.16, No.4, pp.403-414, 1990.

[7] A. Sowmya and S. Ramesh, "Extending Statechart with Temporal Logic," IEEE Trans. Software Eng., Vol.24, No.3, 1998.

[8] A. Gabrielian and M. K. Franklin, "Multilevel Specification of Real-Time Systems," Commun. ACM, Vol.34, No.5, pp.50-60, 1991.