

コンポーネントウェアによる 確率リアルタイムシステムの設計検証手法

小林 さとみ

京都大学

人文科学研究所

satomi@zinbun.kyoto-u.ac.jp

山根 智

金沢大学大学院

自然科学研究科

syamane@is.t.kanazawa-u.ac.jp

コンポーネントウェアによる組込み型システムの設計検証手法を実現するためには、システムはオープンシステムであり、ハイブリッド性があり、不確定性を有するものとして扱う必要がある。本論文では、オープン性、ハイブリッド性、不確定性を扱うために、以下のような理論と技術を開発する。(1)まず、計算モデルとして、コンポーネント同士が入出力動作で同期するモデルを採用する。(2)次に、仕様記述方式として、確率時間インターフェースオートマトンを開発する。(3)最後に、確率時間インターフェースオートマトンの詳細化検証理論として確率時間模倣検証を開発する。ワイヤレス LAN プロトコルの事例により、開発した設計手法の有効性を示す。

1 まえがき

マイクロプロセッサの多くは組込み型システムに使われており、組込み型システムはもっとも重要な計算機システムのパラダイムである。一方、最近、コンポーネントウェアによるシステム開発が有望視されているが、コンポーネントウェアによる組込み型システムの設計手法は確立されていない。なぜならば、組込み型システムのほとんどはリアルタイムシステムであり、制御システムから情報家電までの多岐に渡り、safety-criticalな状況で使われることが多く、大規模化しているからである[1]。本論文では、コンポーネントウェアによる組込み型システムの設計手法を開発する。

組込み型システムの設計を難しくしている要因としては、以下の3つが知られている。

1. オープンシステムとして様々な構成要素が並行に動作していること[2]。
2. デジタルな離散的状態遷移に加えて、タイミング制約や制御法則などのアナログ動作が混在しているといったハイブリッド性があること[3]。
3. 組込み型システムが動作する環境の不確定性があること[4]。

確率オートマトン理論は計算機システムのパラダイムの検証に用いられるが、上述の要因を解決するために、これまで以下の手法が開発されている。

1. コンポーネント同士が入出力動作で同期するモデルが開発されている[5]。
2. デジタル動作とアナログ動作が混在しているシステムの記述のために、時間オートマトンやハイブリッドオートマトンが開発されている[6, 7]。
3. 組込み型システムが動作する環境の不確定性を表現するために、確率オートマトンや確率時間オートマトンが開発されている[8, 9]。

とりわけ、最近、L. de Alfaro や T.A. Henzinger などがアクティブシステム向きのコンポーネントウェアのためのインターフェース理論[10, 11, 12]を研究していることが注目される。彼らのインターフェース理論では、コンポーネントのインターフェースを仕様記述する手段としてインターフェースオートマトンを開発して、ゲーム理論により、そのセマンティックスを定義している。また、彼らは、インターフェースオートマトンの詳細化検証理論として、交互横値検証も開発している。しかし、組込み型システムのコンポーネントウェアによる設計手法を開発するために必要なハイブリッド性や不確定性を考慮していないし、実用的な事例により有効性を示していない。本論文では、時間オートマトンと確率の概念を統合化することにより、以下のような理論と技術を開発して、軽量な形式的手法の考え方により、コンポーネントウェアによる組込み型システムの設計手法を実現する。

- まず、計算モデルとして、コンポーネント同士が入出力動作で同期するモデルを採用する。
- 次に、仕様記述言語として、確率時間インターフェースオートマトンを開発する。
- 最後に、確率時間インターフェースオートマトンの詳細化検証理論として確率時間模倣検証を開発する。

以上の3つの理論と技術を統合化することにより、コンポーネントウェアによる組込み型システムの設計手法の検証方法を実現する。最後に、ワイヤレス LAN [13] の事例により、開発した設計検証手法の有効性を示す。

この論文では次のような構成で、手法の提案とその有効性を示す。2節では、コンポーネントの動作を記述するため、時間オートマトンに確率の概念を追加した確率時間インターフェースオートマトンについて定義する。3節では、シミュレーションによる検証のための確率時間模倣検証を定義する。4節では、ワイヤレス LAN [13] の事例により、開発した設計手法の有効性を示す。最後に、5節では、まとめと今後の課題について述べる。

2 確率時間インターフェースオートマトン

2.1 確率時間インターフェースオートマトンの定義

確率時間インターフェースオートマトンの構文は時間オートマトンの構文を拡張する。まず、離散確率分布を定義する。

(Definition 1) 離散確率分布

有限集合 Q 上の離散確率分布の集合を $\mu(Q)$ と表す。各 $p \in \mu(Q)$ は関数 $p : Q \rightarrow [0, 1]$ である。ただし、 $\sum_{q \in Q} p(q) = 1$ である。

また、時間経過を計測するために、確率時間インターフェースオートマトンはクロック変数を使う。 \mathbf{R} 上のクロック変数の集合を χ とする。 χ 上のクロック制約条件は $x < c$ または $x - y < c$ の布尔結合である。ここで、 c は整数、 $x, y \in \chi$, $<$ は $<$ または \leq である。 χ 上のクロック制約条件の集合を $\Xi[\chi]$ とする。

(Definition 2) 確率時間インターフェースオートマトン

確率時間インターフェースオートマトンは $A = (Q_A, q_A^{init}, \chi_A, Acts_A^I, Acts_A^O, Inv_A^I, Inv_A^O, \rho_A)$ によって定義される。ただし、

- Q_A はロケーションの有限集合である。
- q_A^{init} は初期ロケーションである。
- χ_A はクロック変数の有限集合である。
- $Acts_A^I$ と $Acts_A^O$ は入力アクションと出力アクションであり、 $Acts_A = Acts_A^I \cup Acts_A^O$ とする。
- $Inv_A^I : Q_A \rightarrow \Xi[\chi_A]$ は各ロケーションに入力不变式を割り当てる関数である。
- $Inv_A^O : Q_A \rightarrow \Xi[\chi_A]$ は各ロケーションに出力不变式を割り当てる関数である。
- $\rho_A \subseteq Q_A \times \Xi[\chi_A] \times Acts_A \times \mu(2^{\chi_A} \times Q_A)$ は遷移関係ある。 $(q, g, a, p) \in \rho_A$ に対して、 $q \in Q_A$ は遷移元のロケーション、 $g \in \Xi[\chi]$ は遷移が起きるときのクロック制約条件、 $a \in Acts_A$ は遷移にラベル付けられたアクション、 $p \in \mu(2^{\chi_A} \times Q_A)$ は遷移によってリセットされるクロック集合とロケーション上の確率分布である。

クロック変数の集合 χ の評価は関数 $v : \chi \rightarrow \mathbf{R}$ である。 χ のすべてのクロックに 0 を割り付ける評価を 0_χ と表記する。 χ のすべての評価を $\mathcal{V}(\chi)$ と表記する。評価 $v \in \mathcal{V}(\chi)$ に対して、すべての $x \in \chi$ に対して $(v + \Delta)(x) = v(x) + \Delta$ を $v + \Delta$ によって定義される評価を $v + \Delta$ と表記する。クロックの集合 $r \subseteq \chi$ に対して、 $x \in r$ ならば x に 0 を割り付けてその他ならば $v(x)$ を割り付ける評価を $v[r := 0]$ と表記する。クロック制約条件 $\varphi \in \Xi[\chi]$ に対して、評価 v の下で φ が真ならば、 $v \models \varphi$ と表記する。 $r \subseteq \chi$ に対して、すべての $x \in r$ を 0 で置換することによって φ から得られる条件に対し、 $\varphi[r := 0]$ と表記する。明らかに、 $v[r := 0] \iff v \models \varphi[r := 0]$ である。

2.2 並列合成

リアルタイムシステムでは、システムを構成するコンポーネント同士が同期を取りため、コンポーネントの並列性を記述する必要がある。本節では確率時間インターフェースオートマトンの並列合成の定義について述べる。

もし $Acts_A^O \cap Acts_B^O = \emptyset$ かつ $\chi_A \cap \chi_B = \emptyset$ ならば, 確率時間インターフェースオートマトン A と B は並列合成可能である. それらの共通なアクションは $shared(A, B) = Acts_A \cap Acts_B$ である.

(Definition 3) 並列合成

2つの構成可能な確率時間インターフェースオートマトン A₁ と A₂ に対して, 並列合成 A₁ ⊕ A₂ は以下の要素から構成される :

1. $Q_{A_1 \oplus A_2} = Q_{A_1} \times Q_{A_2}$,
かつ $q_{A_1 \oplus A_2}^{init} = (q_{A_1}^{init}, q_{A_2}^{init})$.
2. $\chi_{A_1 \oplus A_2} = \chi_{A_1} \cup \chi_{A_2}$.
3. $Acts_{A_1 \oplus A_2}^I = Acts_{A_1}^I \cup Acts_{A_2}^I \setminus shared(A_1, A_2)$, かつ
 $Acts_{A_1 \oplus A_2}^O = Acts_{A_1}^O \cup Acts_{A_2}^O$.
4. $Inv_{A_1 \oplus A_2}^I(q_{A_1}, q_{A_2}) = Inv_{A_1}^I(q_{A_1}) \wedge Inv_{A_2}^I(q_{A_2})$, かつ
 $Inv_{A_1 \oplus A_2}^O(q_{A_1}, q_{A_2}) = Inv_{A_1}^O(q_{A_1}) \wedge Inv_{A_2}^O(q_{A_2})$
5. $\rho_{A_1 \oplus A_2}$ は以下の場合がある :

(a) 入出力が同期する場合 :

遷移 $((q_{A_1}, q_{A_2}), g_{A_1} \wedge g_{A_2}, a, r_{A_1} \wedge r_{A_2}, p)$ の集合である. ただし, $p(q_{A_1}, q_{A_2}) = p_{A_1}(q_{A_1}) \times p_{A_2}(q_{A_2})$ である.

(b) 同期しない場合 (その 1) :

遷移 $((q_{A_1}, q_{A_2}), g_{A_1}, a, r_{A_1}, p)$ の集合である. ただし, $p(q_{A_1}, q_{A_2}) = p_{A_1}(q_{A_1})$ である.

(c) 同期しない場合 (その 2) :

遷移 $((q_{A_1}, q_{A_2}), g_{A_2}, a, r_{A_2}, p)$ の集合である. ただし, $p(q_{A_1}, q_{A_2}) = p_{A_2}(q_{A_2})$ である.

3 確率時間模倣検証による詳細化検証手法

詳細化関係は抽象的な仕様と具体的な実装との間を形式化するものであり, 模倣関係が知られている [14]. この関係では, 実装の出力動作が仕様によって許容される動作であることを保証する. しかし, 本論文の確率時間インターフェースオートマトンの詳細化関係では, 実装は仕様よりも多くの入力を受け付けて, 仕様よ

りも小さな出力である必要がある. なぜならば, 仕様が動作する環境ならば実装も動作する必要があるためである.

3.1 確率時間模倣検証の定義

確率時間模倣検証は入出力条件検証と確率時間模倣検証からなる. 確率時間模倣検証に関しては, 我々はすでに実現している [15, 16]. まず, 確率時間インターフェースオートマトンの遷移を定義する.

(Definition 4) 確率時間インターフェースオートマトンの遷移

確率時間インターフェースオートマトン A = $(Q_A, q_A^{init}, \chi_A, Acts_A^I, Acts_A^O, Inv_A^I, Inv_A^O, \rho_A)$ が与えられたとする. 確率時間インターフェースオートマトンの遷移は以下の 2つの遷移の和である.

1. 時間遷移 :

ある $\delta \in \mathbb{R}$ と $\forall \delta' \in \mathbb{R}$ に対して $\delta' \leq \delta$ ならば,
 $< q, v + \delta' > \models Inv_A^I(q)$ または $< v, v + \delta' > \models Inv_A^O(q)$ である.

このとき, $< q, v > \xrightarrow{\delta} < q, v + \delta' >$ である. ただし, $q \in Q_A$, $v \in \mathcal{V}(\chi_A)$ である.

2. 離散遷移 :

$(s, g, a, p) \in \rho_A$ であり, $p(s) > 0$ とする. このとき, $< q, v > \xrightarrow{a, g, p} < q', v[r := 0] >$ である. ただし, $q, q' \in Q_A$, $g \in \Xi[\chi]$, $a \in Acts_A$, $v \in \mathcal{V}(\chi_A)$, $p \in \mu(2^{\mathcal{X}_A} \times Q_A)$ である.

次に, 確率時間模倣関係を定義する.

(Definition 5) 確率時間模倣関係

2つの構成可能な確率時間インターフェースオートマトン A = $(Q_A, q_A^{init}, \chi_A, Acts_A^I, Acts_A^O, Inv_A^I, Inv_A^O, \rho_A)$ と B = $(Q_B, q_B^{init}, \chi_B, Acts_B^I, Acts_B^O, Inv_B^I, Inv_B^O, \rho_B)$ が与えられたとする. なお, A は実装を表して, B は仕様を表すとする. ここで, $S_A = \{< q_A, v_A > | q_A \in Q_A, v_A \in \mathcal{V}(\chi_A)\}$, $S_B = \{< q_B, v_B > | q_B \in Q_B, v_B \in \mathcal{V}(\chi_B)\}$ とする.

以下の条件を満たす二項関係 $R \subseteq S_A \times S_B$ を確率時間模倣関係と呼ぶ.

1. 入出力条件 :

$Acts_B^I \subseteq Acts_A^I$ かつ $Acts_A^O \subseteq Acts_B^O$.

2. 確率時間模倣:

すべての $(q_A, v_A), (q_B, v_B) \in R$ に対して

(a) 時間模倣条件 :

すべての $\delta \in \mathbf{R}$ に対して,

$$< q_A, v_A > \xrightarrow{\delta} < q_A, v_A + \delta > \text{ ならば,}$$

$$< q_B, v_B > \xrightarrow{\delta} < q_B, v_B + \delta > \text{ であり,}$$

$(< q_A, v_A > + \delta, < q_B, v_B + \delta >) \in R$ である.

(b) 確率模倣条件 :

すべての $p_A \in \mu(\{r_A\} \times Q_A)$ に対して,

$$< q_A, v_A > \xrightarrow{p_A} < q_A', v_A' > \text{ ならば,}$$

$$< q_B, v_B > \xrightarrow{p_B} < q_B', v_B' > \text{ であり,}$$

$p_A(< q_A, v_A >) \sqsubseteq_R p_B(< q_B, v_B >)$ である.

ここで, $p_A(< q_A, v_A >) \sqsubseteq_R p_B(< q_B, v_B >)$ とは, 以下の条件を満たすような重み関数 $w : S_A \times S_B \rightarrow [0, 1]$ が存在することである:

i. $\forall s_A \in S_A$ に対して,

$$\sum_{s_B \in S_B} w(s_A, s_B) = p_A(s_A) \text{ である.}$$

ii. $\forall s_B \in S_B$ に対して,

$$\sum_{s_A \in S_A} w(s_A, s_B) = p_B(s_B) \text{ である.}$$

iii. $\forall (s_A, s_B) \in S_A \times S_B$ に対して,

$$w(s_A, s_B) > 0 \text{ ならば } (s_A, s_B) \in R \text{ である.}$$

なお, $(q_A, g_A, \alpha, p_A) \in \rho_A$, $v_A \models Inv_A^\gamma(q_A) \wedge g_A$, $v_A' = v_A[r_A := 0]$, $v_A' \models Inv_A^\gamma(q_A')$ である.

また, $p_B \in \mu(\{r_B\} \times Q_B)$, $(q_B, g_B, \alpha, p_B) \in \rho_B$, $v_B \models Inv_B^\gamma(q_B) \wedge g_B$, $v_B' = v_B[r_B := 0]$, $v_B' \models Inv_B^\gamma(q_B')$ である.

4 コンポーネントベースの設計事例

4.1 ワイヤレス LAN プロトコル

ワイヤレス LAN プロトコル IEEE802.11 [13] は MAC レイヤのプロトコルであり, 通信チャネル割り当てを行うプロトコルである. 大まかなプロトコルの処理は以下であり, 通信チャネル上のデータの流れを図 1 に示す.

1. 通信チャネルが空いる場合:

- (a) 送信端末は DIFS の間, 通信チャネルが空いている (通信が行われていない) か感知する.

- (b) 通信チャネルで通信が行われていないと, 受信端末へ送信を開始する.

- (c) 送信端末の送信終了後に受信端末は SIFS 時間に ACK を返し, 通信を終了する.

2. 通信チャネルが使用されている場合:

- (a) 送信端末はが DIFS の間, 通信チャネルが空いている (通信が行われていない) か感知する.
- (b) 通信チャネルで通信が行われていると, 通信チャネルが空くまで待つ.
- (c) 通信チャネルが空いた後, さらに DIFS の間, 空くか感知する.
- (d) DIFS の間, 通信端末が空いたら, ランダムなバックオフ値を取得する.
- (e) バックオフ値の時間だけさらに通信チャネルが空いてるか感知する.
- (f) バックオフ値の時間だけ通信チャネルが空いていたら, 送信を開始して, SIFS 時間後に, 受信端末が ACK を送信して, それを受け取り, 通信を終了する.

4.2 ワイヤレス LAN プロトコルの仕様記述

本論文では, IEEE802.11 のアドホックネットワークにおける DCF のコンポーネントを確率時間インターフェースオートマトンによりモデル化する. モデルは, 無線 LAN システムは送信端末, 受信端末, 無線媒体から成なり, それぞれ以下のコンポーネントから成る. 送信端末はプロトコル制御コンポーネントとトランスマッショングコンポーネントからなり, 受信端末は受信コンポーネントからなり, 無線媒体はワイヤレスメディアコンポーネントからなる. 本論文の無線 LAN システムのモデルは 2 つの送信端末 送信端末 1, 送信端末 2, 2 つの受信端末 受信端末 1, 受信端末 2, および無線媒体 Wireless Media からなり, モデルのコンポーネント相互関係図は図 2 である. 図 2 では, 各コンポーネント間の信号のやり取りを示している. 矢印の先端で結ばれたコンポーネントに, 矢印の後端側のコンポーネントから出力された矢印の先端側の信号が入力される.

次に, 各コンポーネントを確率時間インターフェースオートマトンにより記述する.

4.3 のプロトコル制御コンポーネント, トランスマッショングコンポーネント, 受信コンポーネントは

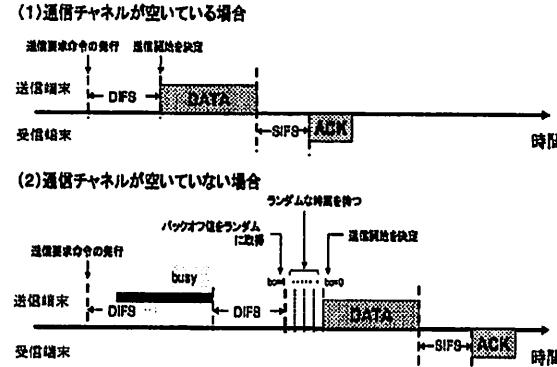


図 1: 通信チャネルでのデータストリーム

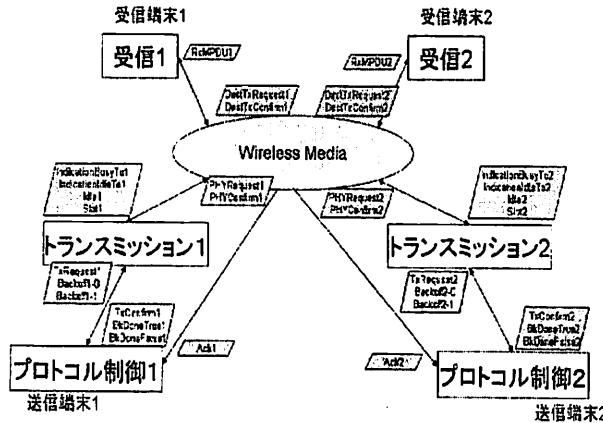


図 2: コンポーネント相互関係図

IEEE802.11 の仕様書 [13] に従って記述を行った。ただし、以下ではプロトコル制御コンポーネントとトランミッションコンポーネントは送信端末 1、受信コンポーネントは受信端末 1 の記述を示すが、送信端末 2、受信端末 2 も同様である。

なお、コンポーネントの图表記では、長方形の中に入力と出力を矢印で記述する。また、確率時間インターフェースオートマトンの图表記では、入力されるアクションには「?」、出力されるアクションには「!」を付けて区別している。

4.3 コンポーネントの仕様と設計

確率時間インターフェースオートマトンによる送信端末 1 のプロトコル制御コンポーネントの仕様 $\text{CONTROL}_1^{(S)}$ を図 3 に示す。

次に、送信端末 1 のプロトコル制御コンポーネントの仕様 $\text{CONTROL}_1^{(S)}$ を詳細化したプロトコル制御コンポーネントの実装を記述した確率時間インターフェースオートマトン $\text{CONTROL}_1^{(I)}$ を図 4 に示す。プロトコル制御コンポーネントの仕様では、データが送信されなかった場合は Drop アクションにより送信エラーを通知する機能があるが、実装では送信エラーを通知する機能は存在しないとする。

確率時間インターフェースオートマトンによる送信端末 1 のトランミッションコンポーネントの仕様

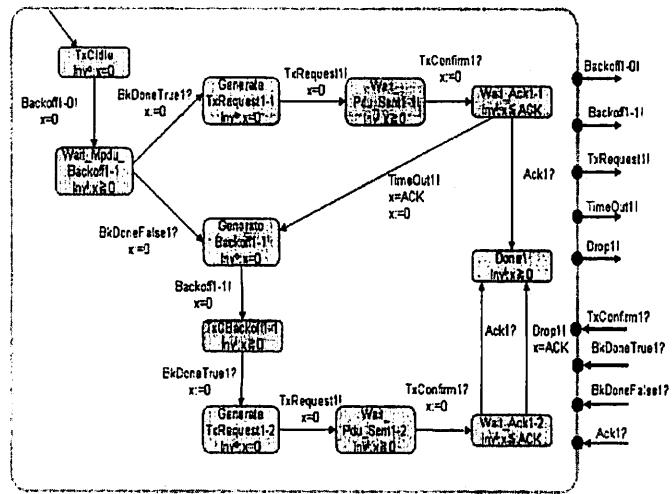


図 3: 確率時間インターフェースオートマトンによるプロトコル制御コンポーネントの仕様 $\text{CONTROL}_1^{(S)}$

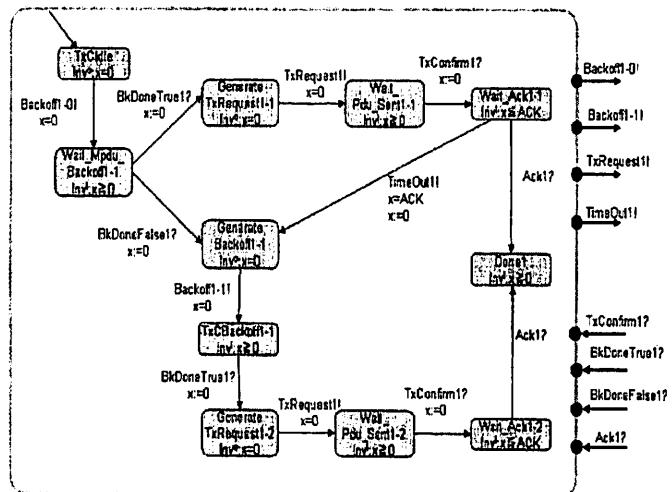


図 4: 図 3 の仕様を実装したプロトコル制御コンポーネンの実装 $\text{CONTROL}_1^{(T)}$

表 2: 検証実験の計測値

選択幅	所要時間	所要メモリ	状態数	遷移数	模倣関係の判定
16	12 時間 52 分 26 秒	874.30MB	29,231	25,030	満たす
8	3 分 20 秒	80.62MB	4,897	5,020	満たす
4	7 秒	11.35MB	1,068	1,308	満たす
2	1 秒	3.18MB	336	468	満たす

表 1: パラメータ設定

スロットタイム	$50\mu s$
SIFS	$28\mu s$
DIFS	$128\mu s$
データタイム	$1000\mu s$
ACK タイム	$205\mu s$
ACK タイムアウト	$300\mu s$

$\text{TRANSMISSION}_1^{(S)}$ 、送信端末 1 のトランスマッシュョンコンポーネントの仕様 $\text{TRANSMISSION}_1^{(S)}$ を詳細化したトランスマッシュョンコンポーネントの実装を記述した確率時間インターフェースオートマトン $\text{TRANSMISSION}_1^{(I)}$ で表す。

仕様のトランスマッシュョンコンポーネントでは、バックオフ時間の取得は $1/8$ ずつの確率分岐でバックオフ時間を取得するようにしたが、実装では、さらに細かく $1/16$ ずつの確率分岐でバックオフ時間を取得するようにした。なお、確率時間インターフェースオートマトンによる記述では、バックオフ時間の取得を離散確率分布上でのロケーションの取得として表現している。

確率時間インターフェースオートマトンによる受信端末 1 の受信コンポーネントの仕様記述を $\text{RECEIVE}_1^{(S)}$ とした。また、受信コンポーネントの実装 $\text{RECEIVE}_1^{(I)}$ は仕様 $\text{RECEIVE}_1^{(S)}$ と等しいとした。

確率時間インターフェースオートマトンによる無線媒体コンポーネントの仕様は $\text{WM}^{(S)}$ とした。なお、無線媒体コンポーネントの実装 $\text{WM}^{(I)}$ は仕様 $\text{WM}^{(S)}$ と等しいとした。

本稿では、周波数ホッピング方式(FHSS)のパラメータを使うことにし、データフレーム送信時間(データタイム)、ACK フレーム送信時間(ACK タイム)、ACK タイムアウト時間(ACK タイムアウト)を表 1 に示す。

4.4 検証実験

検証モデルの無線 LAN システム図 2 は 2 つのプロトコル制御コンポーネント、2 つのトランスマッシュョンコンポーネント、2 つの受信コンポーネント、1 つの無線媒体コンポーネントからなる。

無線 LAN システムの仕様記述は
 $\text{WLAN}^{(S)} = \text{CONTROL}_1^{(S)}$
 $\otimes \text{TRANSMISSION}_1^{(S)} \otimes \text{RECEIVE}_1^{(S)} \otimes \text{WM}^{(S)}$
 $\otimes \text{CONTROL}_2^{(S)} \otimes \text{TRANSMISSION}_2^{(S)}$
 $\otimes \text{RECEIVE}_2^{(S)}$

である。

また、無線 LAN システムの実装記述は
 $\text{WLAN}^{(I)} = \text{CONTROL}_1^{(I)}$
 $\otimes \text{TRANSMISSION}_1^{(I)} \otimes \text{RECEIVE}_1^{(I)} \otimes \text{WM}^{(I)}$
 $\otimes \text{CONTROL}_2^{(I)} \otimes \text{TRANSMISSION}_2^{(I)}$
 $\otimes \text{RECEIVE}_2^{(I)}$

である。

確率時間模倣検証 [15, 16, 17] により、無線 LAN システムの実装記述 $\text{WLAN}^{(I)}$ が無線 LAN システムの仕様 $\text{WLAN}^{(S)}$ を満たすかどうかを検証する。また、実験では、バックオフ時間の選択幅が 16 の場合(確率 $1/16$ の遷移が 16 個)と同様に、8 の場合、4 の場合、2 の場合も検証した。

検証には、Sun Blade 1000(CPU UltraSPARK-900MHz, Main Memory 1024MB) 上の Solaris 8 を用いた。検証実験の所要メモリと所要時間を UNIX の PS コマンドで計測し、得られた計測値を表 2 に示す。どの選択幅の場合も、確率時間模倣関係を満たした。また、検証時に生成される確率時間インターフェースオートマトンの状態数と遷移数も示す。

実験の結果では、確率分布の複雑度以外は同じ条件であるので、確率分布の複雑度に対して、指数オーダーで所要時間と所要メモリが増加していることを示している。選択数が 16 の場合でも所要時間は 13 時間に満たないものであり、全てのケースにおいて、実用的な計算コストで詳細化検証が実行できることがわかる。

5 まとめ

本論文では、確率時間インターフェースオートマトンによるコンポーネントベースの設計手法を構築した。その主要な特徴は以下である：

1. まず、計算モデルとして、コンポーネント同士が入出力動作で同期するモデルを採用した。
2. 次に、仕様記述言語として、確率時間インターフェースオートマトンを開発した。
3. 最後に、確率時間インターフェースオートマトンの詳細化検証理論として確率時間模倣検証を開発した。

さらに、ワイヤレス LAN の事例により、開発した設計検証手法の有効性を示した。今後は、計算モデルとして、確率時間ゲーム理論 [17] を採用して、より形式的で精度の高い設計検証手法に精錬していくことである。

参考文献

- [1] T.A. Henzinger, C.M. Kirsch. Embedded Software: Proceedings of the First International Workshop, EMSOFT '01. LNCS 2211, P.504, Springer-Verlag, 2001.
- [2] D. Harel, A. Pnueli. On the Development of Reactive Systems. *NATO ASI Series F*, Vol. 13, pp.477-498, Springer-Verlag, 1985.
- [3] M.K. Inan, R.P. Kurshan. Verification of Digital and Hybrid Systems. *NATO ASI Series F: Computer and Systems Sciences*, Vol. 170, Springer-Verlag, 2000
- [4] H.A. Hansson. Time and Probability in Formal Design of Distributed Systems. *PhD thesis, Uppsala University*, 1991.
- [5] R. Milner. Communication and Concurrency. *Prentice-Hall*, 1989.
- [6] R. Alur, D.L. Dill. A theory of timed automata. *Theoretical Computer Science*, Vol. 126, pp.183-235, 1994.
- [7] R. Alur, C. Courcoubetis, N. Halbwachs, T.A. Henzinger, Pei-Hsin Ho, X. Nicollin, A. Olivero, J. Sifakis, S. Yovine. The Algorithmic Analysis of Hybrid Systems. *TCS*, Vol.138, No.1, pp. 3-34, 1995.
- [8] R. Segala, N.A. Lynch. Probabilistic Simulations for Probabilistic Processes. *Nordic Journal of Computing*, Vol.2, No.2, pp.250-273, 1995.
- [9] M. Kwiatkowska, G. Norman, R. Segala, J. Sproston. Automatic verification of real-time systems with discrete probability distributions. *Theoretical Computer Science* 282, pp 101-150, 2002
- [10] L. de Alfaro, T.A. Henzinger. Interface Theories for Component-Based Design. *LNCS 2211*, pp.148-165. Springer-Verlag, 2001.
- [11] L. de Alfaro, T.A. Henzinger. Interface Automata. *Proceedings of the Ninth Annual Symposium on Foundations of Software Engineering (FSE)*, pp. 109-120, ACM Press, 2001.
- [12] L. de Alfaro, T.A. Henzinger, M. Stoelinga. Timed interfaces. *LNCS 2491*, Springer-Verlag, pp. 108-122, 2002.
- [13] IEEE. Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications ANSI/IEEE Std 802.11, 1999 Edition.
- [14] R. Milner. An Algebraic Definition of Simulation Between Programs. *IJCAI*, pp.481-489, 1971.
- [15] S. Yamane. Probabilistic Timed Simulation Verification and its application to Stepwise Refinement of Real-Time Systems. *Asian Computing Science Conference*, LNCS 2896, pp.276-290, Springer-Verlag, 2003.
- [16] H. Kodera, S. Yamane. Verification algorithm of probabilistic timed strong simulation of probabilistic timed automata. *RIMS 1426*, pp.133-138, Research Institute of Mathematical Science, Kyoto University, 2005.
- [17] S. Yamane, T. Arai. Design method of embedded systems by probabilistic timed theories. *IEICE Technical Report*, CST2005-23, pp.29-34, 2005.