数理解析研究所講究録
第1691巻 2010年 15-21

コスト付き確率時間オートマトンの抽象化精錬を用いた到達可能性解析手法

安井 雅俊* 山根 智†

1 まえがき

近年, 様々な用途における活躍が期待されている無線センサネットワーク (WSNs) の検証法には需要が存在するが, WSNsの特徴より状態爆発現象が引き起こされるため, WSNs全体としての検証は困難である. WSNsのモデル検査についての研究はほとんど例がない.

関連研究としては, EPITA Research and Development Laboratory の A. Demaille らによる, 確率リアクティブモジュールで WSNs をモデル化し, Approximate Probabilistic Model Checker というツールによって, 近似を行って状態空間の増大を抑え, かつネットワークの特性検証を行ったものがある [1]. しかし, 組込みシステムにおける重要な特性であるリアルタイム性の表現には至っていない. また, University of Twente の J. Berendsen らは, 確率線形ハイブリッドオートマトンのサブクラスであるコスト付き確率時間オートマトンの到達可能性解析 [2] を行っているが, 後方からのゾーングラフ作成による検証であるため, 状態数削減の観点からの研究ではない.

そこで, 本研究では, WSNs をその電力特性をコストで, 不確定性を確率で, リアルタイム性を時間で, 並列動作を並列合成でそれぞれ表現可能であるコスト付き確率時間オートマトンによってモデル化し, WSNs の特性を, コスト境界確率到達可能性問題に帰着する. その上で, 状態爆発を削減することを目的とした検証手法として, コスト付き確率時間オートマトンの抽象化精錬を用いた到達可能性解析手法を提案する.

*金沢大学大学院自然科学研究科
†第1著者に同じ

2 コスト付き確率時間オートマトン

本章では, WSNs のモデル化を行う言語としてコスト付き確率時間オートマトン [2] のシンタックスとセマンティクスを定義する.

2.1 前準備

まず前準備として, WSNs の確率を表現する離散確率分布と, リアルタイム性を表現するクロック変数, 電力特性を表現するコスト変数について定義し, クロック変数とコスト変数を集合で扱うための MP ゾーンも定義する.

定義 1 (離散確率分布)
可算状態集合 $\mathcal{S}$ 上の離散確率分布の集合を $Dist(\mathcal{S})$ で表す. $\mu \in Dist(\mathcal{S})$ は関数 $\mu : \mathcal{S} \to [0,1]$ である. ただし, $\sum_{s\in\mathcal{S}} \mu(s) = 1$ かつ $\{s \mid s \in \mathcal{S} \text{ かつ} \mu(s) > 0\}$ は有限集合である. □

次に, 時間経過を表すクロック変数とクロック変数の評価, クロックの制約を定義する.

定義 2 (クロック変数)
クロック変数は非負の実数値を取る変数であり, 全てのクロックが同じ速度で増加し, 遷移中に 0 にリセットすることが可能である. $\mathbb{R}_{\geq 0}$ 上のクロック変数の集合を $\mathcal{X}$ とする. □

定義 3 (クロック評価)
クロック評価は関数 $\nu : \mathcal{X} \to \mathbb{R}_{\geq 0}$ である. $\mathcal{X}$ の全てのクロック評価の集合は $\mathbb{R}_{\geq 0}^{\mathcal{X}}$ と表す. $\mathbf{0}$ を $\mathcal{X}$ の全てのクロックに 0 を割り当てるクロック評価とする. $X \subseteq \mathcal{X}$ である集合 X に対して, X 内の任意のクロック変数 x を 0 にリセットし, $\mathcal{X}\backslash X$ 内の任意のクロック変数 x は $\nu(x)$ である評価を $\nu[X := 0]$ と表記する. $t \in \mathbb{R}_{\leq 0}$ であるすべての t で $\nu + t$ は, すべての $x \in \mathcal{X}$ に対して, $\nu(x) + t$ の評価を与えるクロック評価とする. □

定義 4 （ゾーン）

$\mathcal{X}$ 上のゾーン ζ はクロック評価の集合 $\mathbb{R}_{\geq 0}^{\mathcal{X}}$ の凸部分集合として以下の構文で帰納的に定義される.

$$\zeta ::= x \leq c | x < c | x \geq d | x > c | x - y \leq d | x - y < d | \zeta \wedge \zeta | true$$

ここで, $x, y \in \mathcal{X}$, $c, d \in \mathbb{N}$ である. なお, $\mathcal{X}$ 上のゾーン ζ の集合を $Zones(\mathcal{X})$ とする. □

クロック評価 ν が, ゾーン ζ を満足するとは, ゾーン中の各クロック変数 $x \in \mathcal{X}$ を ν によって対応するクロック値 $\nu(x)$ によって置き換えた後でクロック評価に関するゾーンの真偽値 $\zeta\nu \in \{true, false\}$ が $true$ であるとき, またその時に限り, $\nu \triangleright \zeta$ と書く.

コスト付き確率時間オートマトンの動作において, 動作開始時からの蓄積コストがあるため通常のゾーンでは状態を記述できない. よって, まず動作開始時からの蓄積コストを表すコスト変数とコスト評価を定義し, コスト付き確率時間オートマトンの動作に現れるクロックとコスト評価の集合をゾーンとそのゾーン上におけるコスト変数の取りうる不等式との連言で定義する.

定義 5 （コスト変数）

コスト変数 z は非負の実数値を取る変数であり, クロックがある速度で増加する際, z はコストの傾きに従って増加する. □

定義 6 （コスト評価）

コスト評価は関数 $c : z \to \mathbb{R}_{\geq 0}$ である. $t \in \mathbb{R}_{\leq 0}$ であるすべての t で $c + nt$ は, コスト変数 z とコストの傾き n に対して, $c(z) + n \cdot t$ の評価を与えるコスト評価とする. □

定義 7 （*Multi-Priced* ゾーン）

Multi-Priced ゾーン（*MP* ゾーン） [2] は $M = \zeta \wedge \phi$ で定義される. ζ はゾーンであり, ϕ は以下の構文で帰納的に定義される.

$$\phi ::= az \bowtie b_1 x_1 + \cdots + b_n x_n + b_0 | \phi \wedge \phi | true$$

ここで, z はコスト変数, $\bowtie \in \{<, \leq, \geq, >\}$, $x_1, \cdots, x_n$ は ζ を構成する全てのクロックであり, $a, b_0, \cdots, b_n \in \mathbb{Z}$ かつ $a > 0$ である. なお, ゾーン $\zeta \in Zones(\mathcal{X})$ 上のコスト式 ϕ の集合を $\Phi(Zones(\mathcal{X}))$ とする. □

クロック評価とコスト評価の組 (ν, c) が, MP ゾーン $M = \zeta \wedge \phi$ を満足するとは,ζ 中の各クロック変数 $x \in \mathcal{X}$ を ν によって対応するクロック値 $\nu(x)$ によって置き換えた後でクロック評価に関するゾーンの真偽値 $\zeta\nu \in \{true, false\}$ が $true$ であるとき, かつ, ϕ 中の各クロック変数 $x \in \mathcal{X}$ とコスト変数 z を組 (ν, c) によって対応するクロック値とコスト値 $\nu(x), c(z)$ によってそれぞれ置き換えた後でクロック評価とコスト評価に関するゾーンの真偽値 $\phi(\nu, c) \in \{true, false\}$ が $true$ であるとき, またその時に限り, $(\nu, c) \triangleright \zeta \wedge \phi$ と書く.

定義 8 （*MP* ゾーン演算）

MP ゾーンを変形する演算を以下に定義する.

$$\begin{aligned}
\mathsf{time_succ}[M, n] &= \{(\nu, c) | \exists t \in \mathbb{R}. \\
&\qquad (\nu - t, c - nd) \triangleright \zeta \wedge \phi\} \\
\mathsf{time_pre}[M, n] &= \{(\nu, c) | \exists t \in \mathbb{R}. \\
&\qquad (\nu + t, c + nd) \triangleright \zeta \wedge \phi\} \\
\mathsf{reset}[M, X] &= \{(\nu[X := 0], c) | (\nu, c) \triangleright \zeta \wedge \phi\} \\
\mathsf{free}[M, X] &= \{(\nu, c) | (\nu[X := 0], c) \triangleright \zeta \wedge \phi\} \\
\mathsf{shift}[M, h] &= \{(\nu, c) | (\nu, c + h) \triangleright \zeta \wedge \phi\}
\end{aligned}$$

また, 入力するゾーンが *MP* ゾーンであるならば, 演算結果も *MP* ゾーンである. □

2.2 コスト付き確率時間オートマトンのシンタックス

定義 9 （コスト付き確率時間オートマトン）

コスト付き確率時間オートマトン P^2TA は, 組 $(L, \bar{l}, \mathcal{X}, inv, prob, \dot{\$})$ で定義される.

- L は各ロケーションの有限集合.
- $\bar{l} \in L$ は初期ロケーション.
- $\mathcal{X}$ はクロックの有限集合.
- 関数 $inv : L \to Zones(\mathcal{X})$ は各ロケーションに不変条件を割り当てる関数.
- $prob \subseteq L \times Zones(\mathcal{X}) \times \mathbb{N} \times Dist(L \times 2^{\mathcal{X}})$ は有限の確率遷移関係.
- $\dot{\$} : L \to \mathbb{N}$ は各ロケーションにコストの傾きを割り当てる関数.

□

定義 10 （コスト付き確率時間オートマトンの *edge*）

コスト付き確率時間オートマトンの *edge* は $(l,g,h,\mu) \in prob$ によって生成され，$\mu(l',X) > 0$ であるような組 (l,g,h,μ,X,l') の形をとる．$\mathrm{edgess}(l,g,h,\mu)$ は (l,g,h,μ) によって生成される *edge* の集合とし，$\mathrm{edgess}(l,g,h,\mu) = \{(l,g,h,\mu,X,l') |$ $(l,g,h,\mu) \in prob$ かつ$\mu(l',X) > 0\}$ であるとする．ここで，$l \in L$, $g \in Zones(\mathcal{X})$, $h \in \mathbb{N}$, $\mu \in Dist(L \times 2^{\mathcal{X}})$ である． □

2.3 コスト付き確率時間オートマトンのセマンティクス

コスト付き確率時間オートマトンのセマンティクスを時間確率システム [3] として定義を行う．時間確率システムはマルコフ決定過程（ＭＤＰ）の形をとり，非決定的な遷移を行う．

定義 11 （時間確率システム）

コスト付き確率時間オートマトン $P^2TA = (L,\bar{l},\mathcal{X},inv,prob,\$)$ の意味である時間確率システム $\mathcal{M}$ はマルコフ決定過程 $(Q,q_0,Steps)$ である．

- 状態集合 $Q \subseteq L \times \mathbb{R}^{\mathcal{X}}_{\geq 0} \times \mathbb{R}_{\geq 0}$
- 初期状態 $q_0 = (l_0,(\nu_0,c_0))$
- 確率遷移関係 $Steps \subseteq Q \times \mathbb{R}_{\geq 0} \times \mathbb{N} \times Dist(Q \times 2^{\mathcal{X}})$

全ての状態 $(l,(\nu,c))$ は $\nu \triangleright Inv(l)$ である，確率遷移関係 $Steps$ は時間遷移と離散遷移からなり，状態 $(l,(\nu,c))$ と組になる確率分布のうち，時間遷移によるものを特に $\mu_\perp$ と表記する，P^2TA の確率遷移関係 $(l,g,h,\mu_P) \in prob$ を $((l,(\nu,c)),t,h,\mu)$ として，以下の様に定める．

- 状態 $(l,(\nu,c))$ からの t 単位時間の時間遷移 $(l,(\nu,c)) \xrightarrow{t,0,\mu_\perp((l',(\nu',c')),\emptyset)} (l',(\nu',c'))$

$$\mu_\perp((l',(\nu',c')),\emptyset) = \begin{cases} 1 & if\ l' = l \wedge \nu' = \nu + t \wedge \\ & \quad c' = c + \dot{\$}(l)t \wedge \\ & \quad \nu' \triangleright inv(l) \wedge t > 0 \\ 0 & otherwise \end{cases}$$

- 状態 $(l,(\nu,c))$ からの確率遷移関係 (l,g,h,μ_P) による離散遷移 $(l,(\nu,c)) \xrightarrow{0,h,\mu((l',(\nu',c')),X)} (l',(\nu',c'))$

$$\mu((l',(\nu',c')),X) = \begin{cases} \mu_P(l',X) & if\ \nu \triangleright g \wedge \\ & \quad \nu' = \nu[X := 0] \wedge \\ & \quad c' = c + h \\ 0 & otherwise \end{cases}$$

□

$\mathcal{M}$ 上の確率遷移関係の確率 $\mu((l',(\nu',c')))$ による遷移は，クロック変数 X をリセットして状態 $(l',(\nu',c'))$ へと到達する遷移である．確率遷移関係の確率分布 μ の標本空間は Q だけでなく Q と $2^{\mathcal{X}}$ との積 $Q \times 2^{\mathcal{X}}$ であるため，P^2TA 上の $\mu_P((l',(\nu',c')),X) > 0$ の一つの遷移が，$\mathcal{M}$ 上の一つの遷移 $\mu((l',(\nu',c')),X) > 0$ に等しく対応している．

時間確率システムのパスは非決定的選択と確率的選択の解決として表現される．時間確率システム $\mathcal{M} = (Q,q_0,Steps)$ のパス ω は以下の様な非空の有限あるいは無限列である．

$$\omega = q_0 \xrightarrow{t_0,h_0,\mu_0(q_1,X_0)} q_1 \xrightarrow{t_1,h_1,\mu_1(q_2,X_1)} \cdots$$

ここで，$0 \leq i \leq |\omega|$ において，$q_i \in Q, (q_i,t_i,\mu_i) \in Steps, \mu_i(q_i) > 0$ である．パス ω の i 番目の状態を $\omega(i)$，i 番目の遷移を $step(\omega,i)$ とし，ω が有限列であるならば，その長さを $|\omega|$，その最後の状態を $last(\omega)$ と表す．状態 q から始まる全ての有限あるいは無限パスの集合を，それぞれ $Path_{fin}(q), Path_{ful}(q)$ と表す．

ここで，非決定性のみ解決する表現として，時間確率システムのアドバサリを導入する．

定義 12 （アドバサリ）

時間確率システム $\mathcal{M} = (Q,q_0,Steps)$ のアドバサリ A [3] は，$\mathcal{M}$ の全ての有限パス ω_{fin} を $(last(\omega_{fin}),\mu) \in Steps$ が存在する離散確率分布 μ に写像する関数である． □

任意のアドバサリ A と状態 q に対して，$Path^A_{ful}(q), Path^A_{fin}(q)$ は，それぞれ A によって生じる $Path_{ful}(q), Path_{fin}(q)$ のサブセットを表すと

し, $Adv_{\mathcal{M}}$ を時間確率システム $\mathcal{M}$ のアドバサリの集合とする. また, パスの最後の状態が等しければパスに依らず全て同じ確率分布を返すアドバサリをシンプルなアドバサリ A_{simple} として区別する. 以降, 単にアドバサリと書くときはシンプルなアドバサリを指す.

アドバサリの下では, 時間確率システムの非決定的な選択は解決される. ここで, 時間確率システム $\mathcal{M} = (Q, q_0, Steps)$ について, 与えられたシンプルなアドバサリ A_{simple} の下での振る舞いはマルコフ連鎖 (MC) [3] によって記述できる.

定義 13 (マルコフ連鎖)

時間確率システム $\mathcal{M} = (Q, q_0, Steps)$ について, 与えられたアドバサリ A の下での $\mathcal{M}$ の振る舞いはマルコフ連鎖 MC^A で記述でき, 組 $(Q^A, q_0^A, \mathbf{P}^A)$ と表す. ここで, 任意の状態 $q, q' \in Q^A$ に対して,

$$\mathbf{P}^A(q, q') = \begin{cases} \mu(q')\ if\ \exists \omega.last(\omega) = q \wedge A(\omega) = \mu \\ 0 \qquad\qquad otherwise. \end{cases}$$

となる. □

次に, アドバサリと関連付けたマルコフ連鎖と時間確率システムに現れるパスの発生確率を定義する.

定義 14 (パスの確率)

時間確率システム $\mathcal{M}$ のアドバサリを A とする. このとき, パスの発生確率 $Prob^A_{fin} : Path^A_{fin} \to [0, 1]$ を以下の様に定義する.

$$Prob^A_{fin}(\omega) = \begin{cases} \mathbf{P}^A(\omega(0), \omega(1)) \cdots \\ \mathbf{P}^A(\omega(n-1), \omega(n)) \quad if\ |\omega| \neq 0 \\ 1 \qquad\qquad otherwise. \end{cases}$$

□

3 コスト境界確率到達可能性解析

本研究では, コスト付き確率時間オートマトンにおける有意な特性の検証を, コスト境界確率到達可能性問題によって考える. コスト付き確率時間オートマトンの動作において, 同じ状態に遷移を行う自己ループが存在するとき, 目的状態に到達するパスが無限数存在する可能性があるため, 動作を調べ上げる必要のあるコスト境界確率到達可能性問題を解くことは困難である. この時, 到達確率の問題を $\leq$ から $>$ の形に制限を加えることで, 有限数のパスを調べることで確率到達可能性問題が検証可能であることが知られている [4]. よって, 本研究では, この問題に対して, コストの制限を加えることで有限数での検証が可能なコスト境界確率到達可能性問題を定義する. 以下に, コスト境界確率到達可能性問題の定義を示す.

定義 15 (コスト境界確率到達可能性問題)

コスト付き確率時間オートマトン $P^2TA = (L, \bar{l}, \mathcal{X}, inv, prob, \$)$ について, コスト境界確率到達可能性問題は, 組 $PPRP = (l_{error}, \lambda', \kappa)$ で定義される. ここで, l_{error} は目標ロケーション, $\lambda' \in [0, 1]$ は目標状態への到達確率, $\kappa \in \mathbb{N}$ は累積コストの上限値である. また, (ν, c) が MP ゾーン $inv(l_{error}) \wedge z > \kappa$ を満足するとき, $(l_{error}, (\nu, c'))$ は目的状態と呼ぶ. このとき, ある $\mathcal{M}$ のアドバサリ $A \in Adv_{\mathcal{M}}$ において, P^2TA の初期状態 $(\bar{l}, (\nu_0, c_0))$ から始まり, $last(\omega) = (l_{target}, (\nu, c'))$ となるパスが一つ以上存在し, そのパスの合計発生確率 P_{max} が条件 $P_{max} > \lambda'$ を満たすとき, かつその時に限り, P^2TA のコスト境界確率到達可能性問題の答えは"*Yes,Reachable*"となり, そうでなければ"*No*"となる. □

4 述語抽象化精錬

WSNs 全体の動作はネットワーク全体を構成するノードの動作モデルを並列合成によって合成することでモデル化できる. 一般に, 実用的な WSNs 内のノード数は数十程度と言われており, 合成したネットワーク全体の動作を記述しても, その状態数は非常に莫大なものとなり, 検証は非常に困難なものとなってしまう. そのため, 計算機のメモリに乗せて現実的に検証可能な状態数になるよう抑え込む必要がある. そこで, 状態空間を抽象化して表現する方法である述語抽象化を導入する [4].

4.1 述語抽象化

述語抽象化は無限状態遷移系の有限の近似を得るために用いられる. この手法は抽象化述語の集合に基づいて抽象化を行う.

定義 16 (抽象化述語)

クロック変数の集合 $\mathcal{X}$ とコスト変数 z において, 述語 ψ は以下のように定義される.

$$\begin{aligned}\psi &::= \psi_{cl} \wedge \psi_{co} \\ \psi_{cl} &::= x_1 \leq c | x_1 < c | x_1 - x_2 \leq d | true \\ \psi_{co} &::= az \leq b_1 x_1 + \cdots + b_n x_n + b_0 | true\end{aligned}$$

ここで, $x_1, x_2, \cdots, x_n \in \mathcal{X}$,$z$ はコスト変数, $c \in \mathbb{N}, a, b_1, \cdots, b_n, d \in \mathbb{Z}$ かつ $a > 0$ である. クロック評価 ν, コスト評価 c, 抽象化述語 $\psi = \psi_{cl} \wedge \psi_{co}$ において, (ν, c) に関する述語 ψ の真偽値を $\psi((\nu, c)) \in \{true, false\}$ とすると, ψ_{cl} に現れるクロック $x \in \mathcal{X}$ に対応する値 $\nu(x)$ を代入した結果が真であり, ψ_{co} に現れるコスト z に対応する値 $c(z)$ を代入した結果が真である, かつその時に限り, (ν, c) は述語 ψ を満たし, $(\nu, c) \models \psi$ と書く. また, 全てのクロック評価 $\nu \in \mathcal{V}_{\mathcal{X}}$ と全てのコスト評価 $c \in \mathcal{V}_z$ において, $(\nu, c) \models true$ とする. □

ロケーション l における抽象化述語の集合 $\Psi^l = \{\psi_1^l, \cdots, \psi_n^l\}$ は, 評価対 (ν, c) から長さ n のビットベクトル b^l へのマッピングである. ここで, 全てのロケーションにおける抽象化述語の集合を $\Psi^{all} = \{\Psi^{l_0} \cup \cdots \cup \Psi^{l_k}\}$ とすると, Ψ^{all} により抽象化関数 α が決定される. b^l の i 番目の要素はロケーション l において $\psi^{l_p}(\nu, c)$ が真となるとき, かつその時に限り真となる. ここで, l における長さ n のビットベクトルは集合 B_n^l の要素であるとし, B_n^l はドメイン $\{0, \cdots, n-1\}$ と変域 $\{0, 1\}$ を持つ関数であると仮定する. また, 全てのロケーションにおけるビットベクトルの集合を $\mathcal{B}$ とする. α の逆像は具体化関数 γ であり, これはビットベクトル b^l を, ビットベクトル b^l の i 番目の要素が真であるときは常に ψ_i^l を満たすような全てのクロック評価に写像する関数である. よって, 具体状態 $(l, (\nu, c))$ の集合は抽象化関数 α によって抽象状態 $\alpha((l, (\nu, c)))$ に写像され, 抽象状態 (l, b^l) は具体化関数 γ により具体状態の集合 $\gamma((l, b^l))$ に写像される. 以下に抽象化, 具体化について定義を行う.

定義 17 (抽象化・具体化)

$\mathcal{X}$ はクロックの集合, $\mathcal{V}_{\mathcal{X}}$ はそれに対応するクロック評価の集合, $\mathcal{V}_{cost}$ はコスト評価の集合であるとする. 述語の有限集合 $\Psi^{all} = \{\Psi^{l_0} \cup \cdots \cup \Psi^{l_k}\}$ が与えられたとき, 抽象化関数 $\alpha : L \times \mathcal{V}_{\mathcal{X}} \times \mathcal{V}_{cost} \to L \times \mathcal{B}$ は以下のように定義される.

$$\alpha((l, (\nu, c)))(i) = (l, \psi_i(\nu, c))$$

また, 具体化関数 $\gamma : L \times \mathcal{B} \to 2^{L \times \mathbb{R}_{\geq 0}^{\mathcal{X}} \times \mathbb{R}_{\geq 0}}$ は以下のように定義される

$$\gamma((l, b^l)) = \{(l, (\nu, c)) \in L \times \mathcal{V}_{\mathcal{X}} \times \mathcal{V}_{cost} \mid inv(l) \wedge \bigwedge_{i=0}^{n-1} \psi_i^l(\nu, c) \equiv b^l(i)\}$$

□

α, γ に関して表記 $\alpha(Q) = \{\alpha((l, (\nu, c))) \mid (l, (\nu, c)) \in Q\}, \gamma(Q^\sharp) = \{\gamma((l, b^l)) \mid (l, b^l) \in Q^\sharp\}$ を用いる. ここで抽象化・具体化関数の対 (α, γ) はガロア接続の形を成す. また, $(l, b^l) \in Q^\sharp$ は抽象状態の集合である.

定義 18 (抽象構造)

具体構造である時間確率システム $\mathcal{M} = (Q, q_0, Steps)$ のオーバー近似である抽象構造 $\mathcal{M}^\sharp = (Q^\sharp, q_0^\sharp, Steps^\sharp)$ を構築する. 抽象構造 $\mathcal{M}^\sharp$ は以下の要素からなる.

- $Q^\sharp = L \times \mathcal{B}$
- $q_0^\sharp = \alpha(q_0)$
- $Steps^\sharp \subseteq Q^\sharp \times Dist(Q^\sharp)$

$((l, b), \mu^\sharp) \in Steps^\sharp$ は $(l, (\nu, c)) \in \gamma((l, b))$ であるような $((l, (\nu, c)), \mu) \in Steps$ が具体構造上に存在するときに限り, 抽象構造上で構築される. ここで, $\mu^\sharp$ は $\mu^\sharp((l', b')) = \mu((l', (\nu', c)))$ である確率分布とする. □

$Steps^\sharp$ には $Steps$ と異なり, 時間遷移であることを示す時間遷移量の定義は存在しないが, $Steps$ で時間遷移を示す確率分布 $\mu_\perp$ から導出される $Steps^\sharp$ の確率分布も区別するために $\mu_\perp^\sharp$ と記す,

また, $\mathcal{M}^\sharp$ のパスは $\mathcal{M}$ のパスと同様に以下である,

$$\omega^\sharp = q_0^\sharp \xrightarrow{\mu_0(q_1^\sharp, X_0)} q_1^\sharp \xrightarrow{\mu_1(q_2^\sharp, X_1)} \cdots$$

4.2 コスト境界確率到達可能性解析

コスト境界確率到達可能性解析は, システムが目標状態 $(l_{target}, (\nu, c))$ へ到達確率 λ より大きい確率で到達できなければ"Not Reachable"を出力し, 到達できれば"Reachable"とその状態へのパス (反例) を出力する. 反例は抽象構造上での初期状態から目

標状態へのパスの集合 $\Omega^{\sharp}_{reach}$ として与えられる．ここで，$\Omega^{\sharp}_{reach}$ の要素であるパスを集めて，その合計到達確率が λ より大きくなる組み合わせのうち要素数が最小となる集合の中で確率最大のものを最小反例 $\Omega^{\sharp}_{smallest} \subseteq \Omega^{\sharp}_{reach}$ [4] と呼び，これを実際の反例として用いる．これは，次に続く反例解析の段階における計算量を削減するためである．

4.3 反例解析手法

4.3.1 準備

ここでは，反例解析に用いる，遷移可能な条件を計算する MP ゾーンの演算を定義する．これは，$\mathcal{M}$ 上で，ある MP ゾーンに含まれる状態において時間遷移，あるいは離散遷移を行うとき，到達可能な状態を含む MP ゾーン，またはその逆を得る MP ゾーン演算である．

- time_pre/succ 演算：時間遷移演算
  time_pre 演算はある MP ゾーンに時間遷移可能な MP ゾーンを計算して，time_succ 演算はある MP ゾーンから時間遷移可能な MP ゾーンを計算する．
  time_pre/succ 演算は定義 8 で定義されている．

- discrete_pre/succ 演算：離散遷移演算
  discrete_pre 演算はある MP ゾーンに離散遷移によって遷移可能な MP ゾーンを計算して，discrete_succ 演算はある MP ゾーンから離散遷移によって遷移可能な MP ゾーンを計算する．

P^2TA の確率遷移関係 $(l, g, h, \mu(l', X)) \in prob$ に対する discrete_pre/succ 演算を，定義 8 を用いて以下の様に定義する．

$$\mathsf{discrete\_succ}[M, g, X, h] = \mathsf{shift}[\mathsf{free}[M, X], h] \wedge g$$

$$\mathsf{discrete\_pre}[M, g, X, h] = \mathsf{reset}[\mathsf{shift}[M, -h] \wedge g, X]$$

4.3.2 反例解析

定義 18 より，抽象構造における遷移は具体構造における遷移のオーバー近似であるため，具体構造に存在する反例は全て抽象構造における反例に含まれるが，その逆は必ずしも成り立たない．言い換えると，反例 $\Omega^{\sharp}_{smallest}$ に従った動作が，具体構造上では実行不可能であることが起こりうる．そのため，抽象構造に対する確率到達可能性解析によって得られた反例が具体構造上に存在するかどうかの判定を行う．

反例解析では，まず得られた反例 $\Omega^{\sharp}_{smallest}$ から反例の要素 $\omega^{\sharp}$ を一つ取り出す．次に，取り出した反例が対応する実際のシステム上で実行可能であるかを調べるパス反例解析を行う．これを $\Omega^{\sharp}_{smallest}$ が空になるまで繰り返し，その後，それらの反例の要素が同一のアドバサリに従って実行することができるかを調べる同時実行反例解析を行う．次に，これらの手順についての詳細な説明を加える．

(i) パス反例解析

まず，反例 $\Omega^{\sharp}_{smallest}$ から要素 $\omega^{\sharp}$ を一つ取り出し，反例の要素が，対応するモデル上で実際に実行可能であるかを調べる．ここでは，抽象構造 $M^{\sharp}$ で得られたパス $\omega^{\sharp}$ がそれぞれ対応する具体構造 $\mathcal{M}$ 上で実行可能であるかを，抽象パスの終端から，目的状態に到達可能な出発条件，到達条件を MP ゾーン演算によって求める，後方反例解析手法を用いて検証する．

(ii) 同時実行反例解析

(i) で反例 $\Omega^{\sharp}_{smallest}$ が空となった場合，解析された反例が同一のアドバサリ条件下で同時に実行可能なのかを検証する．具体構造上のある状態において，時間遷移と離散遷移のどちらを選ぶかは非決定的である．このとき，アドバサリが与えられることによって非決定性が解決され，結果として状態遷移列であるパスが与えられる．一方で抽象構造においては時間が抽象化されているため，到達可能性解析で得られた抽象反例に含まれる抽象パスが具体構造上では同時に実行できない可能性がある．そのため，この同時実行判定解析の段階において得られた反例についてアドバサリが同一であることを調べる．

4.4 精錬

反例解析で偽反例と判定された場合，その反例が存在しないように述語を追加して抽象状態を分割する精錬をおこなう．精錬を行うために必要な情報は，前段階の反例解析の結果から得る．

1) パス反例解析

パス反例解析において反例が偽反例となる場合は，反例 $\Omega^{\sharp}$ の要素であるパス $\omega^{\sharp}$ が具体構造 $\mathcal{M}$ 上で実行不可能である時である．言い換えると，抽象パス $\omega^{\sharp}$ に対応するパスが具体構造上に存在しないことを意味する．このとき，少なくとも $\omega^{\sharp}$ 内の一つの遷移 $q^{\sharp}_i \rightarrow q^{\sharp}_{i+1}$ に対応する具体構造上の遷移 $q \rightarrow q'$ は，遷移可能条件もしくは q' における不変条件を満

たさないため遷移不可能であることが言える．しかし，抽象構造上においては到達可能性解析から実行可能である．これは，ロケーションの遷移可能状態と不可能状態が抽象化によって同一視されているために起きる．故に，抽象状態を述語によって遷移可能な状態と不可能な状態に分割することで反例は実行不可能となる．この状態を分割する述語は，q でのゾーン，及び遷移可能条件，あるいは q' の不変条件から選択する．

2) 同時実行反例解析

同時実行反例解析における判定で偽反例が見つかったとき，任意の同時実行可能なパスがある抽象状態 $q^\sharp$ において異なる遷移先が選択されていることになる．つまり，これを言い換えると，ある状態において時間遷移，離散遷移の異なる遷移が行われているということになる．よって，$q^\sharp$ を時間遷移に関して2つに分割すれば，時間遷移と離散遷移の競合不可能となる．したがって，この境界を示す時間条件を述語として追加する．述語が追加された新たな抽象構造では，さきほどの偽反例は実行不能となる．よって，これを繰り返していくことにより，最終的に正しい確率を計算可能な抽象構造を構築することができる．

5 コスト付き確率時間 CEGAR

述語抽象化，反例による精錬を自動的に検証に適応していく手法が CEGAR の枠組み [5] である．ここでは，コスト付き確率時間オートマトンの検証を目的とした形に CEGAR を拡張したコスト付き確率時間 CEGAR の動作について説明する．

1. Initial Abstraction: 入力であるコスト付き確率時間オートマトン P^2TA と検証問題 $Problem$ から時間確率システム $\mathcal{M}$ と初期述語集合 Ψ^{init} を構築し，それらから初期抽象構造 $\mathcal{M}^\sharp_{\Psi^{init}}$ を構築する．

2. Reachability Analysis: $\mathcal{M}^\sharp_\Psi$ 上で目的となる状態への最大到達可能性確率を計算する．

3. Counterexample Analysis: 2. で目的状態へ到達した反例 $\Omega^\sharp_{smallest}$ の要素をそれぞれについて，パス反例解析，同時実行可能性解析を行って具体構造 $\mathcal{M}$ 上で到達可能かどうかを解析する．

4. Refinement: 3. の反例解析の結果より，2. で得られた反例が存在しないように抽象状態を分割する述語集合 Ψ^{new} を得る．

5. Abstraction: 述語が追加された述語集合 $\Psi' = \Psi \cup \Psi^{new}$ から新たな抽象構造 $\mathcal{M}^\sharp_{\Psi'}$ を得る．

6. 2. に戻る．

このループを繰り返していくことにより，システムが目的状態に"Reach"か，あるいは"Not Reach"かを判定する．"Reach"ならば，目的状態への具体パスが与えられ，この情報をもとにシステムの仕様を変更，改良することが可能となる．

6 まとめ

本論文は，無線センサネットワークを例としたコスト付き確率時間オートマトンのコスト境界確率活性特性について，述語抽象化とその精錬の枠組みを拡張し導入することで，効率的な検証手法を考案した．

参考文献

[1] Akim Demaille. Probabilistic verification of sensor networks. In *In Proc. 4th IEEE Int. Conf. on Comput. Sci., Research, Innovation and Vision for the Future*, pp. 45–54. IEEE Computer Society, 2006.

[2] J. Berendsen, D. N. Jansen, and J. P. Katoen. *Probably on time and within budget:on reachability in priced probabilistic timed automata.* Centre for Telematics and Information Technology, University of Twente, 2006.

[3] M. Kwiatkowska, G. Norman, J. Sproston, and F. Wang. Symbolic model checking for probabilistic timed automata. *LNCS*, Vol. 3253, pp. 293–308, 2004.

[4] 森下篤，駒形龍太，山根智．確率時間 cegar (invited talk)．信学技報，第 109 巻 of *CST2009-5*, pp. 25–30, 2009.

[5] E. M. Clarke. Counterexample-guided abstraction refinement. *LNCS*, Vol. 1855, pp. 154–169, 2000.