ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

NGUYỄN ĐỨC THỌ

KIỂM CHỨNG TỰ ĐỘNG CÁC HỆ THỜI GIAN THỰC XÁC SUẤT

TÓM TẮT LUẬN VĂN

Hà Nội - 2016

Mục lục

MỞ ĐẦU

Đề tài này tập trung vào việc nghiên cứu các đặc tính, mô hình hóa các hệ thời gian thực xác suất và khả năng áp dụng trong việc kiểm chứng mô hình nhằm kiểm chứng tự động các thuộc tính của hệ thời gian thực xác suất bằng công cụ. Phạm vi nghiên cứu của đề tài bao gồm: (1) nghiên cứu các tính chất Markov của các hệ thống, các loại chuỗi Markov và các tính chất của nó; (2) các hệ tự động thời gian thực xác suất và các phương pháp kiểm chứng tự động tính chất của hệ thời gian thực xác suất; (3) nghiên cứ công cụ kiểm chứng mô hình PRISM và khả năng áp dụng trong việc kiểm chứng các tính chất của hệ thời gian thực xác suất, (4) Áp dụng nghiên cứu trong việc mô hình hóa giao thức Alternative Bit Protocol bằng hệ thời gian thực xác suất và thực hiện cài đặt trên công cụ PRISM, thực hiện kiểm chứng tự động các tính chất của hệ thống bằng khả năng kiểm chứng của PRISM.

Chương 1. TỔNG QUAN

Phạm vi đề tài nhằm nghiên cứu các tính chất của ô tô mát thời gian thực xác suất và thực hiện kiểm chứng tự động các tính chất đó bằng công cụ. Có thể phát biểu bài toán kiểm chứng mà đề tài cần giải quyết như sau: Cho hệ thống thời gian thực xác suất M. Thực hiện kiểm chứng tự động bằng công cụ xem M có thỏa mãn tính chất P hay không.

Để có thể giải quyết bài toán kiểm chứng tự động bằng công cụ, phạm vi nghiên cứu của đề tài sẽ tập trung vào các nội dung chính bao gồm:

1. Mô hình hóa hệ xác suất thời gian thực bằng ô tô mát thời gian thực xác suất PTA.
2. Hình thức hóa các tính chất xác suất cần kiểm chứng bằng cây lô gic tính toán xác suất PCTL.
3. Nghiên cứu công cụ hỗ trợ cài đặt PTA và biểu diễn tính chất để thực hiện kiểm chứng tự động.
4. Áp dụng với nghiên cứu với giao thức Alternating Bit Protocol: Mô hình hóa hệ giao thức bằng PTA, hình thức hóa các tính chất bằng PCTL và thực hiện cài đặt hệ giao thức trên công cụ PRISM.
5. Bổ sung: Mô hình hóa và kiểm chứng Hệ điều khiển tự động đóng/mở gác tại điểm giao đường sắt/đường bộ.

Chương 2. CƠ SỞ KHOA HỌC CỦA ĐỀ TÀI

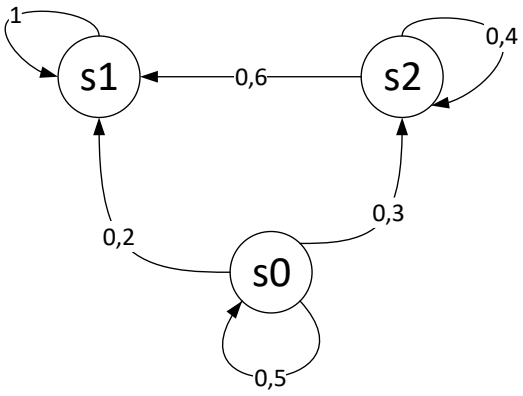
Quá trình có tính chất Markov

Một quá trình là một ô tô mát (hay quá trình, hoặc một chuỗi trạng thái) bắt đầu với một trong các trạng thái này và dịch chuyển từ trạng thái này sang trạng thái khác. Nếu ô tô mát đang ở trạng thái s_i, sau đó chuyển sang trạng thái s_j ở bước tiếp

theo với xác suất được biểu diễn bằng p_{ij}, và giá trị này không phụ thuộc vào các trạng thái ô tô mát trước khi chuyển sang trạng thái hiện tại. Các giá trị xác suất p_{ij} được gọi là các xác suất chuyển (transition probability). Ô tô mát có thể ở trạng thái hiện tại, với xác suất được ghi nhận là p_{ii}. Việc phân bố xác suất các trạng thái ban đầu được định nghĩa bởi S. Thông thường các trạng thái ban đầu được xác định bởi một hoặc một số trạng thái, trong đó nếu các phân bố xác suất chuyển từ trạng thái hiện tại sang các trạng thái tiếp theo chỉ phụ thuộc vào trạng thái hiện tại thì quá trình như vậy được gọi là có tính chất Markov, gọi ngắn gọn là Quá trình Markov.

$$p_{n+1} = Pr(s_{n+1} = x \mid s_1 = x_1, s_2 = x_2, ..., s_n = x_n) = Pr(s_{n+1} = x \mid s_n = x_n)$$

2.1 Xích Markov thời gian rời rạc (DTMC)



Hình 1: Markov chain

Định nghĩa xích Markov thời gian rời rạc DTMC

Chuỗi Markov thời gian rời rạc (gắn nhãn) D là bộ (S, s_0, P, L), trong đó:

- S là tập hữu hạn các trạng thái
- s_0 là trạng thái ban đầu
- P: S x S → [0, 1] là ma trận xác suất, $\sum_{s' \in S} P(s, s') = 1$, mọi s ∈ S
- L: S → 2^{AP} là một nhãn mệnh đề logic với giá trị true tại trạng thái s.

Một hành trình xuyên qua một DTMC là một chuỗi (hữu hạn hoặc vô hạn) các trạng thái ω = s0 s1 s2 … với P(s_i, s_{i+1}) > 0 với mọi i ≥ 0.

Xác suất chuyển từ trạng thái s_i sang s_j sau n bước:

Với **P** là ma trận chuyển của chuỗi Markov. Giá trị thứ ij $p_{ij}^{(2)}$ của ma trận $\mathbf{P}^n$ cho biết xác xuất của chuỗi Markov, bắt đầu tại trạng thái s_i, sẽ ở trạng thái s_j sau n bước chuyển.

Biểu diễn và kiểm chứng tính chất DTMC

Logic PCTL (Probabilistic CTL) thay thế các biểu diễn định lượng của CTL với các toán tử xác suất $\mathcal{P}_{\bowtie\rho}(.)$ với $\rho \in [0,1]$ là ràng buộc xác suất hoặc ngưỡng, và $\bowtie \in \{\leq, <, \geq, >\}$. Cú pháp của mệnh đề logic ϕ của PCTL như sau:

$$\phi ::= \text{true} \mid a \mid \phi \wedge \phi \mid \neg \phi \mid \mathcal{P}_{\bowtie\rho}(\propto)$$

Trong đó $\propto$ là công thức đường (trạng thái tiếp theo $X\phi$ hoặc $\phi_1 \, U \, \phi_2$). Ý nghĩa của toán tử xác suất như sau:

$$s \vDash \mathcal{P}_{\bowtie\rho}(\propto) \text{ nếu và chỉ nếu } Pr_s\{\omega \in Path_s \mid \omega \vDash \propto\} \bowtie \rho$$

được hiểu là xác suất trên các cung đường $\propto$ được tính và so sánh với ràng buộc xác suất, cho giá trị true hoặc false. Lưu ý trong khi $\mathcal{P}_{\geq 0}(\phi_1 \, U \, \phi_2)$ tương đương toán tử tồn tại.

Giải thuật kiểm chứng PCTL thực hiện tương tự như CTL trên ϕ, bằng cách tìm các tập Sat(ϕ) thỏa mãn mệnh đề logic ϕ.

2.2 Quá trình quyết định Markov (MDP)

Định nghĩa Quá trình quyết định Markov MDP

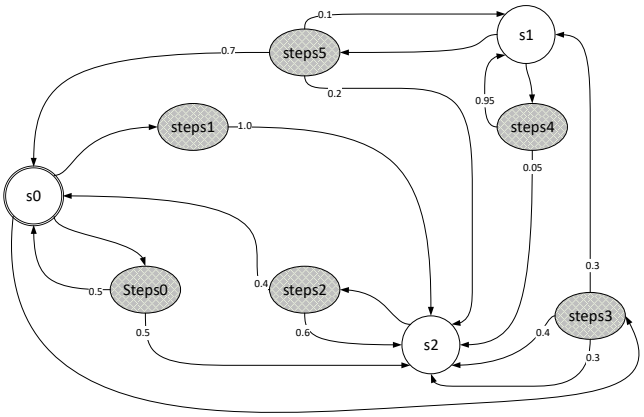
Quá trình quyết định Markov (gắn nhãn) $\mathcal{M}$ là bộ (S, s_0, Steps, L), trong đó:

- S là tập hữu hạn các trạng thái
- s_0 là trạng thái ban đầu
- Steps là một hàm gán mỗi trạng thái $s \in S$ một tập hợp hữu hạn, không rỗng Steps(s) các phân bổ xác suất tại S.
- L: $S \rightarrow 2^{AP}$ là một nhãn mệnh đề logic với giá trị true tại trạng thái s.

Việc thực thi của quá trình quyết định Markov thông qua các thay đổi không xác định và các lựa chọn theo xác suất: khi thuộc một trạng thái cụ thể, hệ thống chọn một cách không xác định một trong các phân bổ xác suất steps $\in$ Steps đối với trạng thái đích. Một hành trình ω của $\mathcal{M}$ là một chuỗi (hữu hạn hoặc vô hạn) các trạng thái

$$s_0 \xrightarrow{\mu 0} s_1 \xrightarrow{\mu 1} s_2 \xrightarrow{\mu 2} \dots$$

Trong đó $s_i \in S$, $\mu_i \in Steps(s_i)$ và $\mu_i(s_{i+1}) > 0$.



Hình 2 Minh họa MDP với 3 trạng thái (s0, s1, s2) và tập các phân bố xác suất Steps (0-5)

Định nghĩa một lập lịch (adversary) của một MDP $\mathcal{M}$ là một hàm A ánh xạ mọi hành trình hữu hạn ω của $\mathcal{M}$ tới một phân bố xác suất A(ω) trên S sao cho A(ω) có giá trị tại trạng thái cuối cùng của ω. Hành vi của MDP $\mathcal{M}$ với một lập lịch đã chọn trước có thể được mô tả bằng một xích Markov rời rạc DTMC P^A, với các trạng thái là các hành trình hữu hạn của $\mathcal{M}$ và xác suất chuyển được cho bởi phân bổ xác suất của A: Với hai hành trình hữu hạn ω, ω', ta có $P^A(\omega, \omega') = A(\omega)(s)$ nếu ω' có dạng $\omega \xrightarrow{A(\omega)} s$ và trong các trường hợp khác thì $P^A(\omega, \omega') = 0$. Vì vậy ta có thể định nghĩa phân bố xác suất Pr_s^A trên tập các hành trình $Path_s^A$ của lập lịch A.

Kiểm chứng tính chất trên các MDP

Logic cây tính toán xác suất (PCTL - Probabilistic Computation Tree Logic) được định nghĩa cho MDPs tương tự DTMC, với sự khác biệt là ngữ nghĩa được tham số hóa bởi lớp Adv các lập lịch và toán tử xác suất chứa các định lượng tường minh.

$s \vDash \text{Adv } \mathcal{P}_{\bowtie \rho}(\propto)$ nếu và chỉ nếu $\Pr^A\{\omega \in \text{Path}^A{}_s \mid \omega \vDash \text{Adv} \propto\} \bowtie \rho$ với mọi lập lịch $A \in \text{Adv}$.

2.3 Xích Markov thời gian liên tục (CTMC)

Xích Markov DTMC và quá trình quyết định Markov MDP chỉ có thể mô hình hóa thời gian rời rạc. Xích Markov thời gian liên tục có các trạng thái là rời rạc, một tham số thời gian trên tập $\mathbb{R}_{\geq 0}$, nhưng không cho phép các lựa chọn bất định. Mỗi quá trình chuyển đổi có một độ trễ ngẫu nhiên phân bố theo cấp số nhân, và một cuộc đua điều kiện được sử dụng để mô tả các dịch chuyển trạng thái đồng thời kích hoạt.

Định nghĩa xích Markov thời gian rời rạc CTMC

Chuỗi Markov thời gian rời rạc (gắn nhãn) C là một bộ (S, s_0, R, L), trong đó:

- S là tập hữu hạn các trạng thái
- s_0 là trạng thái ban đầu

- R: S x S $\rightarrow R_{\geq 0}$ là ma trận tốc độ.
- L: S $\rightarrow 2^{AP}$ là một nhãn mệnh đề logic với giá trị true tại trạng thái s

Việc phân tích các xích CTMC thường dựa trên các trạng thái tức thời tại một thời gian cụ thể và các trạng thái kỳ vọng (trạng thái của CTMC trong thời gian đủ lớn). Xác suất tức thời $\pi_{s,t}(s')$ được định nghĩa là xác suất khi bắt đầu tại s, và ở tại s' tại thời điểm *t*. Xác suất kỳ vọng $\pi_s(s')$ được định nghĩa là giá trị $\lim_{t\rightarrow\infty}\pi_{s,t}(s')$.

Chương 3. KIỂM CHỨNG TỰ ĐỘNG CÁC PTA

3.1 Các định nghĩa cho PTA

Hệ thời gian xác suất (Timed Probabilistic Systems – TPS[1])

Một hệ thời gian xác suất (TPS) T là bộ (S, s0, Act, Steps, lab) trong đó S là tập các trạng thái (có thể vô hạn), s0 $\in$ S là trạng thái ban đầu, Act là tập hữu hạn các hành động, Steps:S x (Act $\cup$ $\mathbb{R}_{\geq 0}$) $\rightarrow$ Dist(S) là hàm xác suất chuyển và lab: S $\rightarrow 2^{AP}$ là hàm gắn nhãn.

Một TPS T bắt đầu từ trạng thái s_0, và khi đang ở s $\in$ S, có một lựa chọn không xác định trước giữa việc thực thi một hành động hoặc để thời gian trôi qua và không hành động gì (letting time pass) a $\in$ (Act $\cup$ $\mathbb{R}_{\geq 0}$) (là lý do Steps(s,a) được định nghĩa). Sau khi lựa chọn được thực hiện (một hành động hoặc cho một khoảng thời gian trôi), trạng thái s' tiếp theo được chọn ngẫu nhiên theo phân bổ xác suất Steps(s,a). Ta giả thiết tại mỗi s $\in$ S, luôn có ít nhất một lựa chọn hành động hoặc để thời gian trôi. Một chuỗi Markov quyết định MDP M là trường hợp đặc biệt của TPS khi bỏ qua yếu tố thời gian trong hàm chuyển, ví dụ hàm chuyển sẽ có dạng $Steps_M$: S x Act $\rightarrow$ Dist(S).

Một đường đi của TPS thể hiện một chuỗi các hành động trên hệ thống, gồm cả các quyết định theo xác suất và quyết định không xác định.

$$\omega = s_0 \xrightarrow{(a0,\mu 0)} s_1 \xrightarrow{(a1,\mu 1)} s_2 \xrightarrow{(a2,\mu 2)} \dots$$

Trong đó $a_{2i} \in \mathbb{R}_{\geq 0}$ và $a_{2i+1} \in$ Act với i $\in \mathbb{N}$.

Ký hiệu ω(i) là trạng thái s_i thứ (i+1) của ω và tổng lũy kế thời gian đến trạng thái ω(i) được xác định bởi

[1] Một số tài liệu gọi là Timed Probabilistic Structures

$$dur_\omega(i) \stackrel{def}{=} \Sigma_{0\le j<i \wedge aj \in \mathbb{R}\ge 0} (a_j)$$

Một vị trí của ω là cặp (i, t) $\in \mathbb{N} \times \mathbb{R}_{\ge 0}$ sao cho $t \le dur_\omega(i+1) - dur_\omega(i)$. Ta gọi vị trí (j, t') là vị trí đứng trước (i,t), ký hiệu (j, t') $\prec$ (i,t), khi j < i hoặc j = i và t' < t.

Để xác định hành vi của PTS T, ta sử dụng ký hiệu *adversary* (lập lịch), trong đó chỉ bao gồm các lựa chọn không xác định. Một cách hình thức, một *adversary* là một hàm từ tập hữu hạn các đường đi với các số chẵn các chuyển dịch tới các khoảng thời gian có thể, và từ tập hữu hạn các đường đi với số lẻ các chuyển dịch tới các hành động có thể thực thi. Với một adversary cố định σ và trạng thái s, ta có thể định nghĩa độ đo xác suất $Pr^{\sigma}_{T,s}$ trên tập hợp $Path^{\sigma}_{T,s}$ của các đường đi không giới hạn xuất phát từ s tương ứng với σ. Với một biến số thực ngẫu nhiên *f* trên $Path^{\sigma}_{T,s}$, ký hiệu $\mathbb{E}^{\sigma}_{T,s}(f)$ là giá trị kỳ vọng của *f* theo phân bổ $Pr^{\sigma}_{T,s}$.

Ta chỉ giới hạn phạm vi xem xét với các adversary có thời gian phân kỳ, ví dụ ta không xét việc thực thi hành động trong đó thời gian không thể vượt qua một giới hạn cụ thể, do những ràng buộc này không phù hợp với một hệ thống thực tế được mô hình hóa. Một cách hình thức, một adversary σ của một TPS T có thời gian phân kỳ nếu

$$Pr^{\sigma}_{T,s}(\{\omega \in Path^{\sigma}_{T,s} \mid \forall c \in \mathbb{N}.\ \exists i \in \mathbb{N}.\ dur_\omega(i) > c\}) = 1.$$

Với mọi trạng thái s thuộc T. Ta ký hiệu Adv_T là tập tất cả các adversary có thời gian phân kỳ của T.

Khi thực hiện các bài toán kiểm chứng với TPS, các đặc tính có thể được xét và kiểm chứng dễ hơn với các cấu trúc thưởng (reward structrure, còn được gọi là chi phí hay giá).

Cấu trúc thưởng (reward structrure)

Một cấu trúc thưởng của TPS T=(S, s0, Act, Steps, lab) là cặp r = (r_S, r_{Act}) trong đó r_S: S$\to\mathbb{R}_{\ge 0}$ là hàm thưởng trên trạng thái và r_{Act}: (SxAct)$\to \mathbb{R}_{\ge 0}$ là hàm thưởng trên hành động.

Với một cấu trúc thưởng r = (r_S, r_{Act}) và hành động s, giá trị $r_S(s)$ xác định tốc độ (theo thời gian) mà giá trị thưởng tích lũy được khi ở trạng thái s. Mặt khác, với trạng thái s và hành động a, giá trị $r_{Act}(s,a)$ xác định giá trị phần thưởng có được khi hành động a được thực thi tại trạng thái s. Một cách hình thức, với đường vô hạn ω = $s_0 \xrightarrow{(a0,\mu 0)} s_1 \xrightarrow{(a1,\mu 1)} \ldots$, phần thưởng tích lũy được trong quá trình dịch chuyển của ω từ trạng thái si đến si+1 được xác định bởi:

$$r(\omega, i) \stackrel{def}{=} \begin{cases} r_S(s_i).a_i \text{ nếu } a_i \in \mathbb{R}_{\ge 0} (tương\ đương\ i\ mod\ 2 = 0) \\ r_{Act}\ (s_i, a_i)\ trong\ các\ trường\ hợp\ khác. \end{cases}$$

Một lựa chọn khác là có thể biểu diễn giá trị giải thưởng tại trạng thái bằng giá trị giải thưởng tại một thời điểm nhất định. Ví dụ có thể áp dụng biểu diễn này trong việc thể hiện số lượng bản tin đang nằm trong hàng đợi tại một thời điểm cụ thể. Khi sử dụng cách diễn dịch này, giá trị thưởng theo hành động sẽ không được xét tới.

Ô tô mát thời gian xác suất PTA

Ô tô mát thời gian xác suất (PTA) mô hình hóa thời gian theo cùng cách ô tô mát thời gian (cổ điển) thực hiện, đó là sử dụng đồng hồ. Đồng hồ là biến thuộc miền thời gian thực không âm, có giá trị tăng như giá trị thời gian thực. Trong các phần tiếp theo, ta giả định có một tập các đồng hồ $\mathcal{X}$. Một hàm v: $\mathcal{X} \rightarrow \mathbb{R}_{\geq 0}$ được gọi là một giá trị đồng hồ, và tập các giá trị của các đồng hồ là $\mathbb{R}_{\geq 0}^{\mathcal{X}}$. Với mọi $v \in \mathbb{R}_{\geq 0}^{\mathcal{X}}$, $t \in \mathbb{R}_{\geq 0}$ và $X \subseteq \mathcal{X}$, gọi v+t chỉ các giá trị đồng hồ của X sau t thời gian kể từ, và v[X:=0] là tập các giá trị đồng hồ, trong đó các đồng hồ thuộc X được đặt về 0.

Tập các ràng buộc thời gian trên tập $\mathcal{X}$, ký hiệu là CC($\mathcal{X}$), được định nghĩa bởi cú pháp:

$$\chi ::= \text{true} \mid x \leq d \mid c \leq x \mid x+c \leq y+d \mid \neg \chi \mid \chi \wedge \chi$$

Trong đó $x, y \in \mathcal{X}$ và $c, d \in \mathbb{N}$. Một giá trị thời gian v thỏa mãn một ràng buộc thời gian χ, ký hiệu $v \vDash \chi$, nếu thay các giá trị của v vào các biến đồng hồ tương ứng thì χ có giá trị *true*. Tập các giá trị thỏa mãn một ràng buộc thời gian được gọi là một vùng. Các ràng buộc thời gian sẽ được sử dụng để định nghĩa cú pháp các PTA và sử dụng trong đặc tả các tính chất của PTA.

Định nghĩa

Một ô tô mát thời gian xác suất (PTA) T là một bộ (L, l0, $\mathcal{X}$, Act, inv, enab, prob, $\mathscr{L}$), trong đó:

- L là tập hữu hạn các vị trí
- $l0 \in L$ là vị trí ban đầu
- $\mathcal{X}$ tập hữu hạn các đồng hồ, có giá trị thực không âm.
- Act là tập hữu hạn các hành động
- inv: L → CC($\mathcal{X}$) là hàm điều kiện ràng buộc
- enab: L x Act → CC(X) là tập các điều kiện thực hiện (các hành động)
- prob: L x Act → Dist(2^{χ} x L) là hàm xác suất chuyển.
- $\mathscr{L}$: L → 2^{AP} là hàm gắn nhãn, ánh xạ mỗi vị trí với một tập các mệnh đề logic.

Ngữ nghĩa của PTA

Cho P = (L, l0, $\mathcal{X}$, Act, inv, enab, prob,$\mathscr{D}$) là một PTA. Ngữ nghĩa của PTA được định nghĩa là một TPS (số trạng thái không giới hạn) TPS [P] = (S, s0, Act, $Steps_P$, lab) trong đó:

- S = {(l,v) ∈ L x $\mathbb{R}^X_{\geq 0}$ | v⊨ inv(l) } và s0 = (l0, {Χ0}), với {Χ0} là trạng thái khởi đầu với tất cả các đồng hồ thuộc Χ có giá trị 0;
- Với mọi (l,v) ∈ S và a∈Act ∪ $\mathbb{R}_{\geq 0}$, ta có $Steps_P$((l,v),a) = λ nếu và chỉ nếu:

  + Dịch thời gian: a∈$\mathbb{R}_{\geq 0}$, v+t'⊨ inv(l) với mọi 0≤t'≤a, và λ = $\mu_{(l,v+a)}$

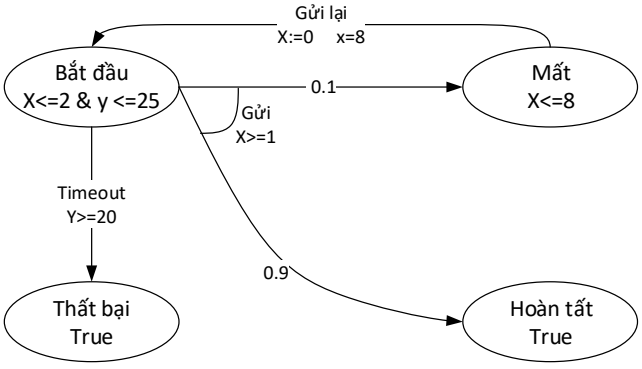
  + Thực thi hành động: a∈Act, v⊨ enab(l,a) và với mỗi (l',v')∈S:

$$\lambda(l',v') = \sum\{|prob(l,a)(X,l')| \; X \in 2^{\chi} \wedge v' = v[X:=0]\}$$

- Với mọi (l,v) ∈S ta có lab (l,v) = $\mathscr{L}$(l)

Ví dụ về PTA

Trong Hình 3, một PTA thực hiện mô hình một giao thức mạng đơn giản. Các bước chuyển là các đường nối giữa các trạng thái. Phân bố xác suất được thể hiện bằng các đường nối xuất phát từ cùng một nơi, và giá trị xác suất được thể hiện trên đường nối. PTA có 2 đồng hồ x và y, được bắt đầu từ giá trị 0. Tại vị trí bắt đầu, hệ thống đợi tối thiểu 1 đơn vị thời gian (thể hiện bằng điều kiện x>=1 tại đường nối khi thực thi hành động Gửi) và tối đa 2 đơn vị thời gian (thể hiện bằng điều kiện x <=2 & y<=25) trước khi gửi một bản tin. Với khả năng 0,9; bản tin được nhận thành công (sang trạng thái Hoàn tất) và khả năng 0,1 bản tin sẽ bị mất (sang trạng thái Mất). Nếu bản tin bị mất, khi x đạt đến 8, PTA trở về trạng thái bắt đầu để chuẩn bị gửi lại bản tin. Hệ thống sẽ chuyển sang trạng thái Thất bại khi tổng thời gian từ khi bắt đầu vượt quá 20 đơn vị (nhưng không quá 25), thể hiện bằng giá trị đồng hồ y.



Hình 3: Minh họa một PTA

Các thưởng của PTA

Các thưởng của PTA P được định nghĩa là cặp r = (r_L, r_{Act}), trong đó r_L: L → $\mathbb{R}_{\geq 0}$ là một hàm gán cho mỗi vị trí tốc độ tích lũy phần thưởng theo thời gian tại vị trí đó, và r_{Act}: L x Act →$\mathbb{R}_{\geq 0}$ là một hàm gán phần thưởng cho mỗi lần thực thi hành động tại vị trí đó.

Cấu trúc thưởng tương ứng trong TPS[P] là r = (r_S, r_{Act}) trong đó $r_S(l,v) = r_L(l)$ và $r_{Act}((l,v),a) = r_{Act}(l,a)$ với $(l,v) \in L \times \mathbb{R}^X_{\geq 0}$ và $a \in Act$.

Mô hình hóa với các PTA

Các biến rời rạc

Việc mở rộng mô hình hóa các PTA với các biến rời rạc giúp thuận tiện trong quá trình mô hình hóa các hệ thống thực. Ta giới hạn việc mở rộng thêm các biến vào PTA chỉ cho số lượng hữu hạn các biến, và các biến thuộc miền giới hạn. Các điều kiện thực thi của PTA có thể tham chiếu đến các biến, và giá trị các biến có thể được cập nhật trong các hành động.

Sự khẩn cấp

Khi mô hình hóa hệ thời gian thực, có thể cần biểu diễn một hành động cần thực thi tức thì tại mộ trạng thái (không cho thời gian trôi qua tại trạng thái đó). Do vậy có thể mô hình hóa sự kiện tức thời trong hệ thống gồm một vài hành động tức thì. Một số cơ chế để mô hình hóa các tình huống này đã được giới thiệu và công bố cho ô tô mát thời gian, như trong ngôn ngữ mô tả hệ thống của công cụ UPPAAL. Dưới đây là một số cách để biểu diễn sự kiện khẩn cấp trong PTA:

- *Vị trí khẩn cấp (urgency)*: là vị trí trong đó không cho phép thời gian trôi qua. Có thể biểu diễn vị trí khẩn cấp trong PTA bằng cách thêm một đồng hồ, trong đó đồng hồ được reset khi vào vị trí, và có ràng buộc giá trị đồng hồ bằng 0 tại vị trí đó.
- *Vị trí cam kết (committed location)*: cũng là vị trí không cho phép thời gian trôi qua, nhưng phải rời khỏi vị trí này ngay khi thành phần khác của hệ thống thực hiện chuyển dịch. Mô tả vị trí cam kết trong PTA có thể thực hiện bằng cách thêm biến logic nguyên tử atom và xây dựng PTA song song. Khi PTA chuyển vào vị trí cam kết, giá trị atom được đặt là true và khi PTA rời khỏi vị trí cam kết, giá trị atom đặt là false, và mọi điều kiện thực hiện của PTA khác được thêm ràng buộc sao cho atom có giá trị false.
- *Hành động khẩn cấp*: là cách thức mô hình hóa các hành động phải được chọn ngay khi điều kiện thực thi thỏa mãn. Việc biểu diễn các hành động khẩn cấp trong cú pháp PTA bằng cách thêm tập con Act_u (của tập hành động Act) để chỉ các hành động khẩn cấp. Sự xuất hiện của các hành động khẩn cấp dẫn đến việc điều chỉnh lại định nghĩa của TPS tương ứng. Với PTA P = (L, l0, χ, Act, inv,

enab, prob,$\mathscr{L}$) với các hành động khẩn cấp Act_u, PTS [P] = (S, s0, Act, $Steps_P$, lab) trong đó S, s0, lab và StepsP((l,v),a) với (l,v) ∈ S và a ∈ Act như trong định nghĩa Ngữ nghĩa của PTA, trong khi với (l,v) ∈ L, t ∈ $\mathbb{R}_{\geq 0}$, ta có StepsP((l,v),t) = $\mu_{(l,v+t')}$ nếu và chỉ nếu:
+ v+t'⊨ inv(l) với mọi $0 \leq t' \leq a$

+ Với mọi $0 \leq t' \leq t$ và a ∈ Act, nếu v+t'⊨ enab(l,a') thì a'∉Act_u

Đặt lại đồng hồ với giá trị bất kỳ: Theo định nghĩa của PTA, các giá trị đồng hồ chỉ được thiết lập lại về 0 khi thực hiện chuyển trạng thái theo xác suất ngẫu nhiên. Tuy nhiên, trong nhiều trường hợp lại cần thiết lập lại giá trị của các đồng hồ về một số nguyên dương. Để mở rộng khái niệm PTA, bổ sung thêm việc đặt lại giá trị đồng hồ về số nguyên dương bất kỳ, định nghĩa PTA cũng được điều chỉnh tương ứng [5].

Tính phân kỳ của thời gian (time divergence)

Sử dụng các khái niệm khác nhau để biểu diễn giá trị thời gian, nhưng các nghiên cứu gần đây chỉ tập trung vào các mục tiêu ký hiệu là Adv[[P]], là những mục tiêu sao cho giá trị biết thời gian luôn vượt qua bất kỳ giá trị ràng buộc nào.

Việc xây dựng và biểu diễn các PTA có thể tạo ra các trạng thái trong đó biến thời gian không thể tiến lên bất cứ giá trị nào, các trạng thái này được gọi là khóa thời gian (timelock) trong cài đặt các ô tô mat thời gian, và được coi là lỗi trong quá trình mô hình hóa hệ thống. Các trạng thái bị khóa thời gian có thể được xác định nhờ quá trình phân tích mô hình kiểm chứng, và có thể được loại bỏ khỏi mô hình bằng cách điều chỉnh các ràng buộc về thời gian và các điều kiện chuyển.

3.2 Đặc tả tính chất cho các PTA (properties specification for PTAs)

Định nghĩa:

Cú pháp logic mô tả tính chất PTA được cho bằng các văn phạm sau:

$$\phi \quad ::= \quad \text{true} \mid a \mid \chi \mid \phi \wedge \phi \mid \neg\phi \mid P_{\bowtie q}\,[\Psi] \mid R^{r}_{\bowtie q}\,[\rho]$$

$$\Psi \quad ::= \quad \phi\ U^{\leq k}\ \phi \mid \phi\ U\ \phi$$

$$\rho \quad ::= \quad I^{=k} \mid C^{\leq k} \mid F\ \phi$$

Trong đó a ∈ AP là mệnh đề nguyên tử, $\chi \in CC(\chi)$ là một ràng buộc thời gian, toán tử so sánh ⋈ ∈ {≤, <, ≥, >}, p ∈ $\mathbb{Q} \cap [0,1]$, q ∈ $\mathbb{Q}_{\geq 0}$, r là cấu trúc thưởng và k ∈ $\mathbb{N}$.

Đây là các mệnh đề logic mở rộng với các toán tử logic xác suất (P) và các toán tử phần thưởng (R). Diễn giải không chính thức, tính chất được biểu diễn dạng $P_{\bowtie q}$

[Ψ] cho biết xác suất để công thức Ψ là đúng luôn thỏa mãn ràng buộc ⋈q. Tính chất biểu diễn dạng $R^r_{\bowtie q}$ [ρ] cho biết giá trị kỳ vọng của hàm giải thưởng ρ trong cấu trúc thưởng r thỏa mãn ràng buộc ⋈q.

Đặc tả tính chất của PTA được bổ sung thêm 2 công thức: ràng buộc theo thời gian (công thức có dạng $\phi_1 \, U^{\leq k} \, \phi_2$) và không ràng buộc thời gian (công thức có dạng $\phi_1 \, U \, \phi_2$). $\phi_1 \, U \, \phi_2$ có nghĩa là một trạng thái s thỏa mãn ϕ_2 và mọi thời gian trước đó thì ϕ_1 được thỏa mãn. $\phi_1 \, U^{\leq k} \, \phi_2$ có ý nghĩa tương tự, nhưng yêu cầu sự kiện ϕ_2 thỏa mãn phải trước thời điểm k. Một số toán tử hữu ích cũng có thể được bổ sung, bao gồm $F \, \phi \equiv true \, U \, \phi$, có nghĩa ϕ sẽ được thỏa mãn, và $F^{\leq k} \, \phi \equiv true \, U^{\leq k} \, \phi$ cho biết ϕ sẽ được thỏa mãn trước thời điểm k. Ta cũng có $G \, \phi \equiv \neg(F \, \neg\phi)$, cho biết ϕ luôn thỏa mãn, và $G^{\leq k} \, \phi \equiv \neg(F^{\leq k} \, \neg\phi)$ cho biết ϕ được thỏa mãn liên tục đến thời gian k.

Toán tử giải thưởng $R^r_{\bowtie q}$ [ρ], tương ứng ρ với các giá trị I=k tham chiếu đến giá trị phần thưởng tại thời điểm tức thời k, C≤k tham chiếu đến tổng phần thưởng tích lũy đến thời điểm k, và F ϕ tham chiếu đến tổng giải thưởng tích lũy đến khi đạt đến một trạng thái thỏa mãn ϕ. Một cách hình thức, các ngữ nghĩa của logic được định nghĩa như sau:

Định nghĩa

Cho P là một PTA, [P] = (S, s0, Act, $Steps_P$, lab) là một ngữ nghĩa của P, và r là cấu trúc phần thưởng trên [P], tương ứng với cấu trúc phần thưởng trên P. Cho trạng thái s=(l,v) ∈ S, quan hệ thỏa mãn ⊨ được định nghĩa quy nạp như sau:

$s \models true$		s luôn luôn đúng
$s \models a$	⇔	a ∈lab (s)
$s \models \chi$	⇔	$v \models \chi$
$s \models \phi 1 \wedge \phi 2$	⇔	$s \models \phi 1 \wedge s \models \phi 2$
$s \models \neg\phi$	⇔	$s \not\models \phi$ (s không thỏa mãn ϕ)
$s \models P_{\bowtie q} \, [\Psi]$	⇔	$Pro^{\sigma}_{[P],s} \, (\{\omega \in Path^{\sigma}_{[P],s} \mid \omega \models \Psi\}) \bowtie \rho$ với mọi $\sigma \in Adv[P]$
$s \models R^r_{\bowtie q} \, [\rho]$	⇔	$\mathbb{E}^{\sigma}_{[P],s} \, (rew(r, \rho)) \bowtie q$ với mọi $\sigma \in Adv[P]$

trong đó:

$\omega \models \phi_1 \, U^{\leq k} \, \phi_2$	⇔	tồn tại một vị trí (i,t) của ω sao cho $\omega(i) + t \models \phi_2$ và $dur_\omega(i)+t \leq k$ và $\omega(i) + t' \models \phi_1 \vee \phi_2$ với mọi vị trí (j,t') trước (i,t) của ω

$\omega \vDash \phi_1 \, U \, \phi_2$ $\Leftrightarrow$ tồn tại một vị trí (i,t) của ω sao cho $\omega(i) + t \vDash \phi_2$ và $\omega(i) + t' \vDash \phi_1 \vee \phi_2$ với mọi vị trí (j,t') trước (i,t) của ω

Ví dụ về các tính chất thường được kiểm chứng của PTA có dạng thức logic được thể hiện như sau:

- $P_{\geq 0,8}[F^{\leq k} \, ack_n]$ – "Xác suất bên gửi nhận được n ack trong k đơn vị thời gian tối thiểu là 0.8"
- Trigger $\rightarrow P_{<0.0001}[G^{\leq 20} \neg deploy]$ – "Xác suất để túi khí không bung ra trong vòng 20 mili giây chắc chắn nhỏ hơn 0.0001"
- Pmax = ?[¬sent U fail] – "Xác suất tối đa khi lỗi xảy ra trước khi bản tin gửi thành công là bao nhiêu"
- R^{time}_{max} = ? [F end] – "Xác suất tối đa giao thức có thể hoàn tất"
- $R^{pwr}_{<q}$ [$C^{\leq 60}$] – "Tổng mức năng lượng tiêu thụ trong 60 giây đầu tiên <q"

3.3 Các phương pháp kiểm chứng tự động PTA

Với bài toán tổng quát về kiểm chứng các tính chất Φ của PTA P, ví dụ xác định $Sat(\Phi) = \{s \in S | \, s \vDash \Phi \}$: tập các trạng thái S của P thỏa mãn tính chất P. Hiện đã có nhiều kỹ thuật kiểm chứng PTA được công bố, và các kỹ thuật này hỗ trợ các loại biểu thức logic khác nhau. Ta cùng xem các kỹ thuật kiểm chứng mô hình với PTA đã được nghiên cứu và công bố.

- Đồ thị miền
- Đồ thị miền biên
- Phương pháp đồng hồ số
- Phương pháp đạt được lùi
- Trừu tượng hóa và làm mịn với trò chơi ngẫu nhiên

Hai kỹ thuật đầu tiên nêu trên dựa trên khái niệm Đồ thị miền, ban đầu được xây dựng cho việc đánh giá khả năng quyết định và mức độ phức tạp của bài toán kiểm chứng mô hình hơn là để triển khai thực hiện kiểm chứng. Các phương pháp khác khá hiệu quả trong việc kiểm chứng mô hình cho một số loại biểu thức logic cụ thể. Bảng 1 thể hiện khả năng kiểm chứng của các phương pháp khác nhau với các loại biểu thức logic.

Bảng 1: Tổng hợp kỹ thuật kiểm chứng và khả năng áp dụng

Loại biểu thức	Đồ thị miền	Đồ thị miền biên	Đồng hồ số (với các PTA đóng)	Phương pháp đạt được lùi	Trò chơi ngẫu nhiên

Biểu thức đơn $P_{\bowtie q}$ [Ψ]	✓	✓	✓	✓	✓
Biểu thức đơn $R^r_{\bowtie q}$ [ρ]	X	✓	✓	Đang mở	Đang mở
Biểu thức không chứa $R^r_{\sim q}$[ρ]	✓	✓	X	✓	Đang mở
Logic đầy đủ	X	X	X	Đang mở	Đang mở

Trừ phi được nêu cụ thể các ngoại lệ, ta giả thiết PTA P không có khóa thời gian và được cấu trúc sao cho đảm bảo thời gian không giới hạn.

3.3.1 Phương pháp đồng hồ số (digital clock method)

Phương pháp đồng hồ số, trong đó giới hạn các ngữ nghĩa thời gian liên tục của PTA sao cho mọi dịch chuyển thời gian luôn có giá trị là 1 đơn vị. Do vậy các giá trị của đồng hồ là các số nguyên (thay vì số thực). Từ ràng buộc này và giá trị hằng số c_x đã biết, là giá trị hằng số lớn nhất mà tất cả các đồng hồ phải so sánh trong P và các thuộc tính ϕ, ta có thể xây dựng một MDP hữu hạn trạng thái để biểu diễn PTA.

Phương pháp đồng hồ số có thể áp dụng để kiểm chứng các tính chất dạng $P_{\bowtie p}[\Psi]$ và $R^r_{\bowtie q}[\rho]$ mà không có chứa các biểu thức dạng $P_{\bowtie p}[\Psi]$ và $R^r_{\bowtie q}[\rho]$ trong các biểu diễn công thức của Ψ và ρ. Nó có thể sử dụng để kiểm chứng trong các trạng thái với các giá trị đồng hồ so sánh với các số nguyên. Tính chính xác của phương pháp đồng hồ số cũng dựa trên giả thiết P và ϕ là đóng, theo nghĩa tất cả cả các ràng buộc rạng $x \leq d$ hoặc $d \leq x$ được chứa trong một số chẵn các phép phủ định. Ngoài ra, tất cả các ràng buộc thời gian và điều kiện chuyển của P được giả định không có liên hệ đường chéo, theo nghĩa các ràng buộc rạng $x+c \leq y+d$ không được chấp nhận.

Với một giá trị của đồng hồ $v \in \mathbb{N}^{\mathcal{X}}$, ký hiệu $v \oplus 1$ là giá trị đồng hồ sao cho $(v \oplus 1)(x) = \min\{v(x) + 1, c_x + 1\}$ với mọi $x \in \mathcal{X}$. Ngữ nghĩa đồng hồ của P và ϕ được định nghĩa như ngữ nghĩa chuẩn, ngoại trừ giới hạn thời gian chuyển có giá trị là 1, và mỗi giá trị đồng hồ x có thể tăng tới giá trị tối đa c_x+1. Một cách hình thức, ngữ nghĩa đồng hồ số của một PTA P đóng được định nghĩa là một MDP hữu hạn trạng thái $Dgt(P, \phi) = (S, (l0, 0), Act \cup \{l\}, Steps, lab)$ trong đó:

- $S = \{(l,v) \in L \times \mathbb{N}^{\mathcal{X}} \mid v \vDash inv(l) \wedge (\forall x \in \mathcal{X}.\ v(x) \leq c_x + 1)\}$;
- $Steps((l,v),a) = \lambda$ nếu và chỉ nếu:
  + Dịch chuyển thời gian: $a=1$, $v \oplus 1 \vDash inv(l)$ và $\lambda = \mu(l, v \oplus 1)$;
  + Thực thi hành động: $a \in Act$, $v \vDash inv(l, a)$ và, với mọi $(l', v') \in S$
    $$\lambda(l',v') = \Sigma\{|prob(l,a)(X, l') \mid X \in 2^{\mathcal{X}} \wedge v' = v[X:=0]\ |\};$$
- $lab(l,v) = \mathcal{L}(l)$ với mọi $(l,v) \in S$.

Số lượng các trạng thái trong ngữ nghĩa đồng hồ số được giới hạn bởi giá trị $|L|.\Pi_{x\in\mathcal{X}}(c_x+1)$.

Việc kiểm chứng các tính chất có dạng $P_{\bowtie p}[\Psi]$ và $R^{r}_{\bowtie q}[\rho]$ thực hiện trực tiếp trên MDP hữu hạn trạng thái. Với công thức $P_{\bowtie p}[\Psi]$, việc tính toán thực hiện tương tự như Đồ thị miền đã nêu. Với công thức $R^{r}_{\bowtie q}[F\ \phi]$ và cấu trúc thưởng $r=(r_{Act}, r_L)$ của PTA, ta xây dựng cấu trúc thưởng mới $r'=(r'_S, r'_{Act})$ trong đó $r'_S(l,v) = 0$, $r'_{Act}((l,v),l) = r_L(l)$ và $r'_{Act}((l,v),a) = r_{Act}(l,a)$ với mọi $(l,,v) \in S$ và $a \in Act$. Sau đó sử dụng các giải thuật của MDP để tính giá trị kỳ vọng lớn nhất và nhỏ nhất của giải thưởng khi đạt đến tập thỏa mãn $Sat(\phi)$. Trường hợp $\rho = C^{\leq k}$ và $\rho = I^{=k}$, sử dụng phương pháp giản lược thuộc tính để tính.

3.3.2 Phương pháp đạt được lùi (backward reachability)

Phương pháp đạt được lùi không áp dụng cho các tính chất có dạng $R^{r}_{\bowtie q}[\rho]$. Phương pháp này dựa trên thủ tục tìm vị trí tiền nhiệm, từ tập các trạng thái S', liệt kê danh sách các trạng thái từ đó có thể đến S' bằng cách để thời gian trôi hoặc thực thi hành động. Tập các trạng thái được biểu diễn là các trạng thái biểu tượng, $z = (l, \zeta)$, bao gồm vị trí l và một ràng buộc thời gian ζ trên tập $\mathcal{X}$, biểu diễn tập các trạng thái $\{(l,v) \mid v \vDash \zeta\}$.

Trước hết, thực thi thủ tục tìm vị trí tiền nhiệm thực hiện tham số hóa các hành động và các cạnh của PTA. Khi duyệt qua các nhánh, biểu đồ về các node được xây dựng và các node tạo nên các trạng thái biểu tượng, và mỗi cạnh được bổ sung từ trạng thái biểu tượng z tới trạng thái biểu tượng z' nếu z được sinh ra từ z' bằng thủ tục tìm vị trí tiền nhiệm. Cạnh (z, z') được đánh nhãn tương ứng với hành động trong cạnh PTA. Các trạng thái biểu tượng được sinh ra không phải là thành phần của không gian trạng thái PTA.

Sau khi việc duyệt thủ tục tìm tiền nhiệm kết thúc, biểu đồ thu được có thể được sử dụng để xây dựng nên một MDP hữu hạn trạng thái. Để xây dựng các hàm chuyển trạng thái xác suất, thông tin phải được tổng hợp từ nhiều trạng thái biểu tượng để có thông tin chính xác về các cạnh PTA (ứng với một hành động cụ thể của PTA). Việc này thực hiện bằng cách tính các điểm giao của các trạng thái biểu tượng có ít nhất một cạnh đi ra khỏi trạng thái có chung nhãn, khi đó bổ sung cạnh tương ứng vào trạng thái biểu tượng mới tạo.

Cách tiếp cận như trên chỉ áp dụng được với các thuộc tính dạng $P_{\bowtie p}[\Psi]$ trong đó $\bowtie \in \{\leq, <\}$, chẳng hạn như phép tính xác suất lớn nhất trong PTA. Với các trường hợp $\bowtie \in \{\geq, >\}$, phương pháp tính cần phải điều chỉnh, và chỉ áp dụng cho các PTA thời gian không phân kỳ.

3.3.3 Làm mịn trừu tượng với trò chơi ngẫu nhiên (abstraction refinement with stochastic games)

Phương pháp làm mịn trừu tượng với trò chơi ngẫu nhiên có thể kiểm chứng các tính chất dạng $P_{\bowtie p}[\Psi]$ bằng cách tính xác suất đạt đến trạng thái nào đó. Phương pháp này sử dụng khái niệm trò chơi dựa trên trừu tượng hóa các đầu vào của MDP và áp dụng các kỹ thuật làm mịn. Phương pháp này có thể áp dụng với các PTA có các ràng buộc không liên hệ đường chéo, do một trong các thủ tục thực hiện là thăm dò khả năng đạt đến phía trước, và các thủ tục này chỉ có thể thực hiện khi PTA không có ràng buộc đường chéo.

Ý tưởng triển khai là xây dựng một MDP trừu tượng, với dạng trò chơi hai người. việc khái quát hóa MDP để thể hiện có hai dạng không xác định khác nhau, mỗi dạng được điều khiển bởi một người chơi khác nhau. Trong phương pháp này, người chơi một điều khiển các quyết định trong MDP trừu tượng, và người chơi hai điều khiển các quyết định trong MDP ban đầu. Một giải thuật tối ưu xác suất trong trò chơi ngẫu nhiên (ví dụ xác suất tối đa người chơi 1 đạt mục tiêu, trong khi người chơi 2 đang cố hạn chế nó) có thể tạo ra các giới hạn dưới và giới hạn trên cho xác suất đạt đến của MDP ban đầu.

Cơ chế làm mịn trừu tượng được giới thiệu trong [] cung cấp cách thức tạo ra trò chơi trừu tượng tự động, bằng cách duyệt qua các lớp trừu tượng đến khi giới hạn trên và giới hạn dưới có độ lệch dưới ngưỡng ε xác định. Kỹ thuật này có thể giúp xác định xác suất (lớn nhất hoặc nhỏ nhất) của PTA với trạng thái nào đó. Trước hết, xây dựng biểu đồ chạm tới cho các trạng thái (reachability graph), dựa trên các thủ tục duyệt các trạng thái tiếp theo (có thể chạm tới được từ trạng thái hiện tại) bằng cách thực thi hành động hoặc để thời gian trôi. Từ đây, một trò chơi ngẫu nhiên trừu tượng đã được tạo ra thông qua các trạng thái biểu tượng cho đến khi các xác suất cần tính toán đạt đến giá trị yêu cầu.

3.3.4 So sánh các phương pháp kiểm chứng

Về hiệu suất và khả năng mở rộng, phương pháp đồng hồ số đã được chứng minh hoạt động tốt trong thực tế, nhưng hiệu năng hạn chế khi có số lượng lớn các đồng hồ hoặc có nhiều hằng số xuất hiện trong ràng buộc thời gian; trong những tình huống này, các phương pháp còn lại đã cho thấy hoạt động hiệu quả hơn. Các kỹ thuật tổng hợp thông số có thể sử dụng để giảm số lượng các hằng số trong các ràng buộc thời gian của các lớp con của PTA, và cho các tính chất xác suất không có ràng buộc thời gian. Một kỹ thuật khác cũng được áp dụng để tăng hiệu năng là sử dụng cài đặt biểu tượng (dựa trên biểu đồ quyết định nhị phân).

Cài đặt ban đầu của Phương pháp đạt được lùi cho thấy nó tạo ra MDP tương đối nhỏ, tuy nhiên giải thuật này có chi phí triển khai lớn. Kết quả thực tế của phương pháp làm mịn trừu tượng với trò chơi ngẫu nhiên cho thấy hiệu năng tốt hơn cả. Tuy

nhiên, các phương án tối ưu sau đó được đưa ra cho Phương pháp đạt được lùi giúp cải thiện hiệu năng đáng kể, và cải thiện cho phương pháp làm mịn trừu tượng với trò chơi ngẫu nhiên trong rất nhiều trường hợp.

Chương 4. CÔNG CỤ KIỂM CHỨNG MÔ HÌNH PRISM

Từ phiên bản 4.0 (Tháng 5/2011), công cụ PRISM bắt đầu hỗ trợ kiểm chứng mô hình PTA, bên cạnh các mô hình DTMC, CTMC, MDP đã có trước đó. Tính đến tháng 9/2016, phiên bản PRISM mới nhất là 4.3. Các phương pháp kiểm chứng các tính chất của PTA được cài đặt trong PRISM từ phiên bản 4.0 tới nay là phương pháp đồng hồ số, Phương pháp đạt được lùi và phương pháp trừu tượng hóa với trò chơi ngẫu nhiên.

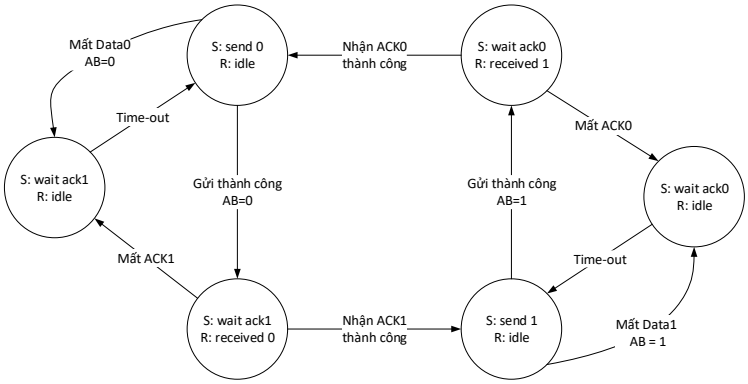
Mô hình hóa PTA

PRISM sử dụng ngôn ngữ mô hình hóa đồng nhất cho tất cả các mô hình xác suất được hỗ trợ, gồm cả PTA. Để hỗ trợ PTA, PRISM từ phiên bản 4.0 trở đi đã bổ sung loại dữ liệu mới là **clock** cho các biến đồng hồ. Các biến đồng hồ có thể xuất hiện trong các biểu thức điều kiện, trong các vế trái của lệnh, và có thể được reset như các biến thông thường khác. Từ khóa mới **invariant** được bổ sung để biểu diễn càng ràng buộc thời gian tại trạng thái. Hình [] là ví dụ đoạn mã PRISM dùng để biểu diễn PTA tương ứng, trong đó có chứa cấu trúc thưởng với nhãn là energy, được sử dụng để thể hiện tốc độ tích lũy giải thưởng là 2.5 tại trạng thái s=0.

Các kĩ thuật kiểm chứng trong PRISM

PRISM phân tích hai lớp tính chất chính của PTA: (1) Xác suất lớn nhất, nhỏ nhất để đạt tới một mục tiêu nào đó, có thể kèm ràng buộc thời gian (ví dụ: “xác suất lớn nhất của túi khí không bung trong vòng 0.02 giây”); và (2) Giá trị kỳ vọng lớn nhất/nhỏ nhất của giải thưởng tích lũy được khi đạt tới một mục tiêu nào đó (ví dụ: “Kỳ vọng thời gian tối đa để giao thức hoàn tất”). Hiện nay các phương pháp kiểm chứng đồng hồ số, Phương pháp đạt được lùi và phương pháp trò chơi ngẫu nhiên đã được cài đặt, trong đó phương thức trò chơi ngẫu nhiên là cấu hình mặc định của PRISM cho các mô hình PTA.

Chương 5. KIỂM CHỨNG GIAO THỨC ABP BẰNG PRISM



Hình 4: Biểu đồ mô tả trạng thái Bên gửi, Bên nhận trong giao thức ABP

5.1 Mô hình hóa giao thức bít luân phiên bằng PTA

Một số giả thiết đối với hệ thống

Không làm mất tính tổng quát của việc thực hiện mô hình hóa hệ thống, ta có một số giả thiết như sau:

- Tin nhắn được gửi tức thời trên đường truyền (không có độ trễ).
- Bên nhận có cơ chế kiểm tra để biết bản tin được gửi có bị hỏng hay không (chẳng hạn dùng check sum), và với các bản tin hỏng, bên nhận sẽ bỏ qua, không xử lý gì. Do vậy có thể coi bản tin bị hỏng, bị sai lệch như bản tin bị mất trên đường truyền, và khi nói bản tin gửi đến bên nhận sẽ là các bản tin chính xác từ nguồn gửi.
- Phía gửi luôn tin tưởng bản tin đã được chuyển tới đầu kia chính xác (và chuyển sang trạng thái chờ), dù thực tế bản tin có thể bị hỏng, mất trên đường truyền. Tuy nhiên phía chờ có giới hạn thời gian nhận ack tương ứng với một bản tin đã gửi (timeout) để xác định bản tin cần truyền lại.
- Phía nhận tin tưởng bản tin ACK đã được gửi chính xác tới người gửi (và chuyển sang trạng thái nghỉ), dù thực tế có thể bản tin đã mất, hỏng.
- Phía nhận không gửi lại hai bản tin giống nhau liên tục cho dòng Dữ liệu ra nếu không nhận được một bản tin khác ở giữa, ví dụ B sẽ không gửi 2 bản tin Data ứng với ACK1 liên tiếp nếu giữa 2 lần gửi không có 1 bản tin Data ứng với ACK0. Cơ chế này giúp dòng dữ liệu ra không bị nhận các bản tin lặp do cơ chế gửi lại.

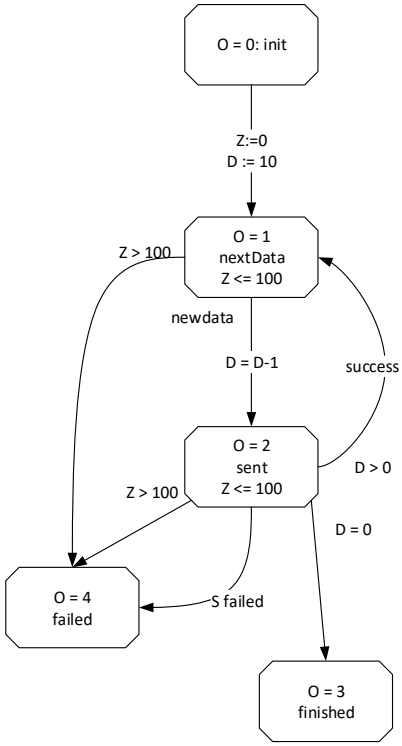
Sử dụng các ô tô mát thời gian xác suất để mô hình một hệ thống gửi tin gồm:

- Nguồn dữ liệu (O): Là nguồn gửi và cần truyền thông điệp sang bên nhận. Thông điệp là khối dữ liệu gồm D bản tin (ví dụ: D = 10), lần lượt các bản tin được chuyển đến Bên gửi để gửi sang Bên nhận. Các bản tin chỉ được gửi nếu bản tin trước đó có kết quả là Thành công. Việc gửi được coi là Kết thúc (thành công) nếu tất cả các bản tin được gửi thành công trong thời gian TIMEOUT cho trước,

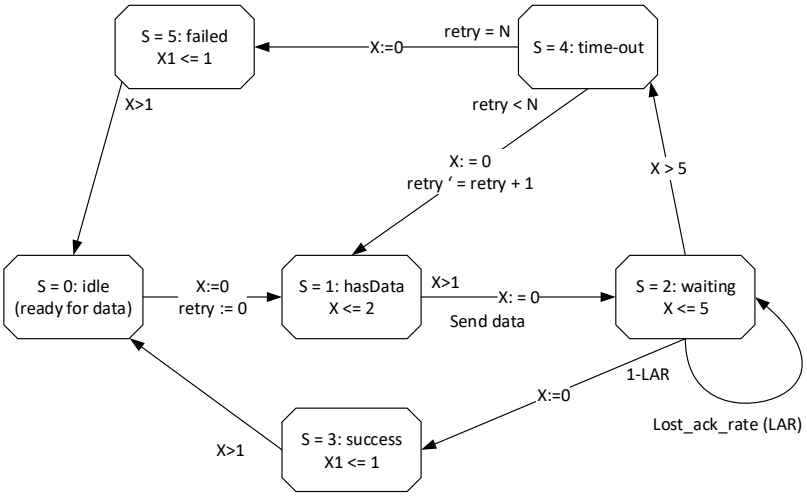
ngược lại nếu một trong các bản tin không thành công hoặc tổng thời gian gửi tin vượt quá giới hạn định trước (ví dụ: TIMEOUT > 100), hệ thống sẽ ngừng gửi và việc gửi tin là thất bại.

- Bên gửi (S): Bên gửi nhận lần lượt từng gói dữ liệu vào và gửi sang Bên nhận theo giao thức ABP. Mỗi lần gửi tin, có một số bản tin không đến được Bên nhận, hoặc đến nhưng giá trị alternating bit không khớp, gọi là bản tin không thành công. Tỉ lệ các bản tin không thành công khi gửi được thể hiện bằng tham số LOST_DATA_RATE. Sau khi nhận gói tin từ Nguồn dữ liệu, thời gian S cần xử lý và gửi tin trong thời gian 1-2 (1 <= x <= 2). Sau khi gửi tin, S sẽ chờ nhận ACK từ R. Nếu sau khoảng thời gian ACK_TIMEOUT định trước (ví dụ: ACK_TIMEOUT = 5) không nhận được ACK thì S sẽ:
    - (i) hoặc gửi lại bản tin nếu số lần gửi lại còn nhỏ hơn số RETRY cho trước;
    - (ii) hoặc coi việc gửi bản tin là thất bại và không gửi lại bản tin đó nữa.
    - Khi xác định trạng thái gửi tin là Thành công hay Thất bại, S có khoảng thời gian nghỉ 1-2 đơn vị trước khi chuyển về trạng thái sẵn sàng để gửi bản tin tiếp theo.
- Bên nhận (R): Mỗi khi nhận được bản tin từ Bên gửi, Bên nhận mất 1 đến 2 đơn vị thời gian để xử lý bản tin (1 <= y <=2), sau đó chuyển sang trạng thái gửi ACK về bên nhận. Việc gửi ACK cũng mất 1-2 đơn vị thời gian. Sau khi đã gửi ACK, R chuyển về trạng thái nghỉ để sẵn sàng nhận bản tin tiếp theo. Khi R gửi ACK, có một tỷ lệ nhất định bản tin sẽ mất trên đường truyền hoặc bị sai lệch khi đến đích. Tỉ lệ này được thể hiện bởi tham số LOST_ACK_RATE.

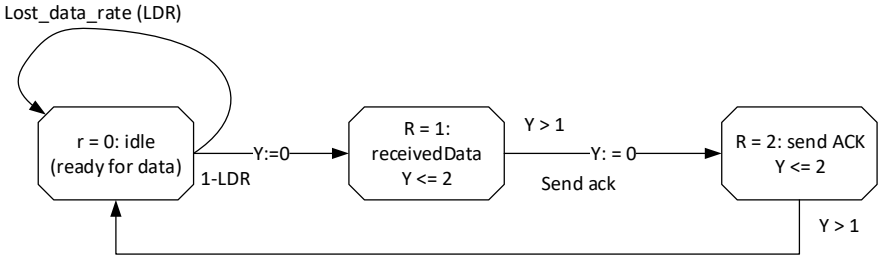
Từ các đặc tả trên, ta có các thành phần trao đổi bản tin của hệ thống là các ô tô mát thời gian xác suất, và cả hệ thống gồm các PTA được biểu diễn bằng các biểu đồ chuyển trạng thái như biểu diễn trong Hình 7, Hình 8 và Hình 9 (trình các hình này, giả thiết: TIMEOUT = 100; ACK_TIMEOUT = 5; DATA = 10):



Hình 5: Biểu đồ trạng thái của nguồn gửi trong quá trình truyền tin



Hình 6: Biểu đồ trạng thái của bên gửi trong quá trình truyền tin



Hình 7: Biểu đồ trạng thái của bên nhận trong quá trình truyền tin

Các đặc điểm xác định trước của hệ thống:

- Xác suất mất gói tin của đường truyền: LOST_DATA_RATE;
- Xác suất mất bản tin ack của đường truyền: LOST_ACK_RATE;
- Số lần retry của một gói: RETRY;
- Thời gian time-out của cả hệ thống: TIMEOUT;
- Thời gian time-out chờ nhận ACK_TIMEOUT;
- Số lượng bản tin cần truyền DATA;

5.2 Cài đặt hệ truyền tin sử dụng giao thức bít luân phiên bằng công cụ PRISM

Mã cài đặt PTA của hệ truyền tin bằng giao thức bít luân phiên trong công cụ PRISM (xem chi tiết trong đề tài)

Các tính chất của hệ sẽ được kiểm chứng với các đặc điểm xác định trước của hệ thống:

- Xác suất lớn nhất để hoàn thành việc truyền dữ liệu thành công là bao nhiêu?
  Pmax = ? [F “finished”]
- Xác suất lớn nhất khi truyền dữ liệu thành công trong T thời gian là bao nhiêu?
  Pmin = ? [F <= T “finished”]
- Xác suất lớn nhất bị mất gói tin là bao nhiêu?
  Pmax = ? [F “lost”]
- Xác suất lớn nhất bị mất gói tin trong thời gian T là bao nhiêu?
  Pmax = ? [F <=T “lost”]

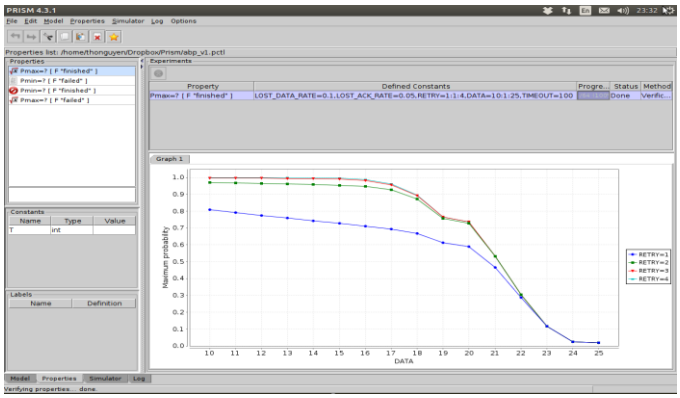
5.3 Kết quả kiểm chứng và các đánh giá

5.3.1 Pmax = ? [F “finished”]

Kết quả kiểm chứng của PRISM với các tham số:

LOST_DATA_RATE = 0.1; LOST_ACK_RATE = 0.05; RETRY = 1..4; DATA = 10..24

Biểu đồ kết quả kiểm chứng được ghi nhận tại hình 10.



Hình 8: Pmax = ? [F "finished"]

Nhận xét:

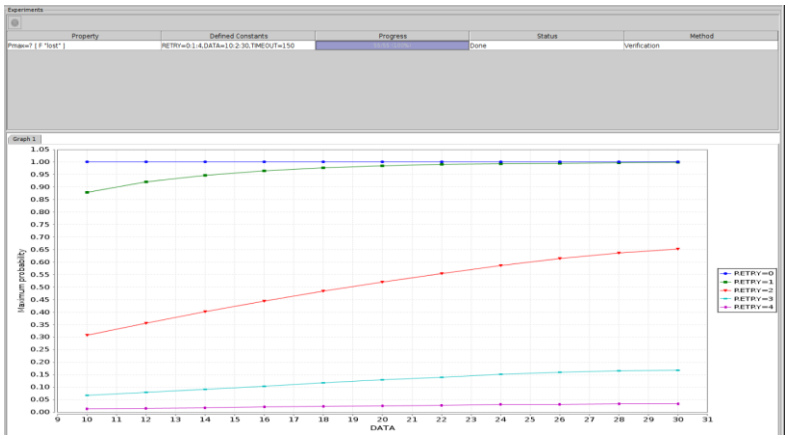
- Xác suất gửi bản tin thành công tăng thêm khi số lần RETRY tăng thêm, tuy nhiên các giá trị RETRY >=3 không có khác biệt đáng kể, do giới hạn TIMEOUT = 100 của hệ thống.

5.3.2 Pmax = ? [F “lost”]

Kết quả kiểm chứng của PRISM với các tham số:

+ LOST_DATA_RATE = 0.1; LOST_ACK_RATE = 0.1; TIMEOUT = 150; ACK_TIMEOUT = 5; RETRY = [0..4]; DATA = [10..30]

Biểu đồ kết quả kiểm chứng được ghi nhận tại Hình 11.



Hình 9: Pmax = ? [F "lost"]

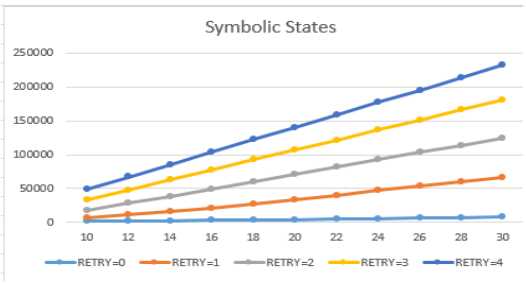
- Việc tăng số lượng retry giúp giảm nhanh khả năng mất gói tin trong quá trình truyền tin.

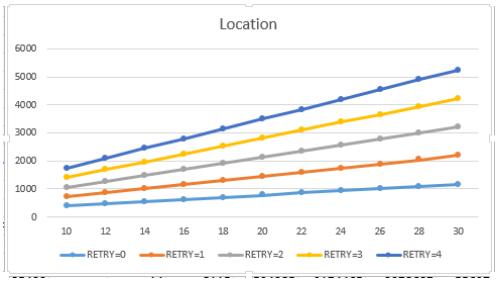
Sử dụng phương thức kiểm chứng đạt được lùi, khi xây dựng MDP, dữ liệu Bảng 2 ghi nhận kích thước của MDP (số lượng trạng thái, số lượng dịch chuyển và số lượng lựa chọn của MDP) đều tăng tuyến tính theo tất cả các giá trị hằng số.

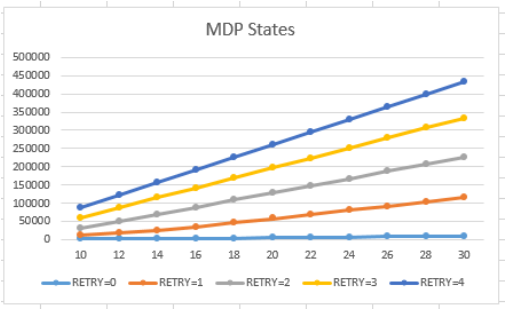
Bảng 2 Quy mô tính toán khi DATA = 10..30; RETRY = 0..4

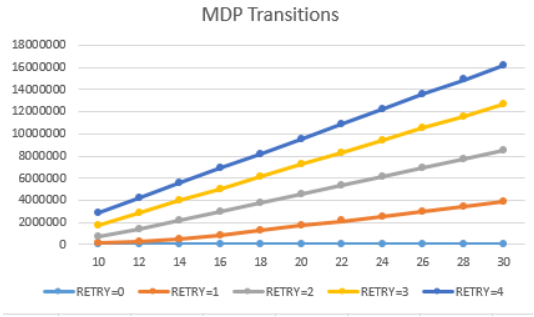
DATA	RETRY	LOCATION	SYMBOLIC STATES	MDP STATES	MDP TRANSITIONS	MDP CHOICES
10	0	393	1499	1929	4155	5204
20	0	783	4199	5459	18115	20814
30	0	1173	8099	10589	49875	54824
10	1	731	7313	12093	151531	155739
20	1	1461	33874	58409	1696183	1714641
30	1	2191	66334	115279	3922873	3958631
10	2	1069	18160	32082	709856	719914
20	2	2139	71076	128455	4563017	4601332
30	2	3209	124946	226655	8543937	8610992
10	3	1407	33408	60587	1787875	1806138
20	3	2817	107128	197051	7244923	7302566
30	3	4227	180848	333521	12701983	12799006
10	4	1745	48799	89680	2894619	2921125

20	4	3495	140549	260890	9565009	9640555
30	4	5245	232299	432100	16235399	16359985









KẾT LUẬN

Trong phạm vi đề tài, giao thức bít luân phiên đã có thể được mô hình hóa và kiểm chứng định lượng các tính chất xác suất lớn nhất. Đề tài có thể tiếp tục phát triển và thực hiện so sánh hiệu năng, kích cỡ các MDP khi kiểm chứng giao thức bít luân phiên bằng các phương thức kiểm chứng khác nhau.

TÀI LIỆU THAM KHẢO

1. Charles M. Grinstead (Swarthmore College, USA), J. Laurie Snell (Dartmouth College, USA) (2003), *Introduction to Probability* (2nd edition), American Mathematical Society, Chapter 11.Markov Chains, pp.405-470. http://www.dartmouth.edu/~chance/teaching_aids/books_articles/probability_book/book.html , freely redistributed under the terms of the GNU Free Documentation License (FDL).

2. D.V.Hung, M.Zhang, On verification of probabilistic timed automata against probabilistic duration properties, in: 13th IEEE International Conference on Embedded and Real-time Computing Systems and Applications (RTCSA 2007), 21-24 August 2007, Daegu, Korea, 2007, p.165-172

3. Gethin Norman, David Parker and Jeremy Sproston (2013), Springer, Model Checking for Probabilistic Timed Automata. *Formal Methods in System Design*, 43(2), pp.164-190
4. Sheldon M.Ross (University of Southern California, USA) (2010), *Introduction to Probability Models (Tenth Edition)*, Elsevier, Chapter 4.Markov Chains, p.191-291; Chapter 6. Continuous-Time Markov Chains, pp.371-420.
5. Marta Kwiatkowska, Gethin Norman (University of Birmingham, UK), Roberto Segala (Università di Verona, Italy), Jeremy Sproston (University of Birmingham) (2002), *Theoretical Computer Science*, Elsevier, Automatic verification of real-time systems with discrete probability distributions, pp.101-150
6. Marta Kwiatkowska, M., Norman, G., Sproston, J.,Wang, F.: Symbolic model checking for probabilistic timed, automata. Information and Computation 205(7), 1027–1077 (2007)
7. Rajeev Alur and David L.Dill (Computer Science Department, Standford University, USA) (1994), Theoretical Computer Science, A theory of timed automata, pp.183-235.
8. Van Hung Dang, Miaomiao Zhang, Dinh Chinh Pham (2015), VNU Journal ò Science, Towards Model-checking Probabilistic Timed Automata against Probabilistic Duration Properties.