OSTIS-2015
(Open Semantic Technologies for Intelligent Systems)

УДК 007:519.816

ВЕРИФИКАЦИЯ МОДЕЛЕЙ ПРОЦЕССОВ В ДИНАМИЧЕСКИХ СИСТЕМАХ ПО МЕТОДУ MODEL CHECKING

Королев Ю.И.

Национальный исследовательский университет «МЭИ»,
г. Москва, Россия

KorolevYu@gmail.com

Рассматриваются средства моделирования процессов в сложных динамических системах в плане их использования в интеллектуальных системах поддержки принятия решений реального времени. В качестве формального аппарата предлагается использовать сети Петри специального типа – раскрашенные (colored) сети Петри реального времени с поддержкой темпоральной логики Аллена. Обуславливается необходимость верификации моделей, разработанных с помощью данного формализма, предлагается использование метода верификации Model Checking. Работа выполнена при финансовой поддержке РФФИ и Фонда содействия инновациям.

Ключевые слова: интеллектуальная система поддержки принятия решений, моделирование процессов, сети Петри, темпоральная логика, верификация систем.

Введение

Интеллектуальные системы поддержки принятия решений реального времени (ИСППР РВ), предназначенные для помощи оперативно-диспетчерскому персоналу (лицу или группе лиц, принимающих решения, ЛПР) при управлении сложными динамическими объектами или процессами [Вагин и др., 2001], относятся к классу динамических интеллектуальных систем (ДИС) [Осипов, 2008]. Понятие динамической системы применяется в ситуациях, когда исследуется вопрос, как система (объект) развивается во времени посредством установления взаимосвязи между значениями параметров системы в различные моменты времени. Такой подход необходим при изучении и моделировании поведения многих сложных технических, организационно-технических, социальных, экологических систем, в частности, энергетических и транспортных систем [Еремеев и др., 2010]. Возникающие в таких системах зависимости и связи, зачастую в условиях различного типа неопределенности (так называемых НЕ-факторов или «зашумленных» данных) могут быть очень сложными и плохо формализуемыми, описываться качественными параметрами, а законы функционирования задаваться с использованием эмпирических или экспертных знаний. Все это не допускает традиционного аналитического представления и моделирования поведения системы. Таким образом, в ДИС типа ИСППР РВ необходимо наличие специальных средств моделирования, которые могут быть использованы и для моделирования процессов и в самой ДИС. В качестве эффективного средства моделирования и анализа процессов динамических систем предлагается использовать аппарат цветных сетей Петри реального времени с поддержкой темпоральной логики Аллена (РСП РВ ТЛА) [Еремеев и др., 2013]. Надежность и предсказуемость поведения подобных систем зачастую являются более важными свойствами, чем производительность, модифицируемость и т.п. Кроме того, использование сетей Петри подразумевает достаточно высокий уровень параллелизма, что, как и учет темпоральных зависимостей, требует наличия средств анализа и верификации моделей, созданных на его основе данного аппарата.

1. Анализ модели

Многопоточные программы, характерные для многих систем управления, в том числе, реального времени типа ИСППР РВ, крайне подвержены ошибкам. Хорошо известно, что даже в тех случаях, когда функционирование каждой из параллельных взаимодействующих компонент системы абсолютно ясно, человеку трудно понять работу всей системы в целом. Такие системы годами могут сохранять «тонкие» ошибки, проявляющиеся в исключительных ситуациях. Рассматриваемый

подкласс РСП РВ ТЛА представляет собой визуальный язык программирования [Еремеев и др., 2013] с формально определенным синтаксисом. Модели, разработанные с помощью этого аппарата, кажутся полностью формализованными. Однако с точки зрения семантики это не так: из самой модели не следует непосредственно полное формальное описание ее поведения. Параллелизм, присущий сетям Петри в целом, и учет темпоральных зависимостей, введенный для упрощения разработки, зачастую делают целостное восприятие процесса более сложным. Поэтому для анализа поведения и верификации моделей, построенных с помощью РСП РВ ТЛА, необходимо использовать дополнительные инструменты.

Известны три основных группы методов анализа сетей Петри: основанные на построении графов изменения состояний; матричные методы, использующие уравнения сети и инварианты; методы редукции. При работе с раскрашенными сетями Петри последние две группы методов используются редко из-за высокой сложности формальных определений подобных подклассов. В [Еремеев и др., 2014] в качестве основного инструмента анализа РСП РВ ТЛА предлагается использовать графы покрытия (ГП). При этом для состояний сети (пары (M, S), где M – маркировка сети, а S – вектор временных меток мест) вводится бинарное отношение покрытия. Два состояния покрывают друг друга, если их маркировки совпадают, а временные метки либо совпадают, либо не превышают максимального возраста доступа места, то есть такого значения темпоральной метки, когда фишки-токены становятся доступными для всех выходных переходов места. При этом удовлетворяются условия рефлексивности, симметричности и транзитивности, следовательно отношение покрытия есть отношение эквивалентности (~) на множестве $R(M_0,S_0)$ – множестве всех состояний, достижимых из начальное состояние сети (M_0,S_0). При построении ГП после определения нового состояния сети необходимо проверить, есть ли в графе вершина, которая отображает состояние, покрывающее новое. Если есть, то необходимо добавить только новую дугу, которая идет к найденной вершине. В противном случае вершина нового состояния добавляется в ГП вместе с соответствующей дугой. Таким образом, каждая вершина ГП помечена элементом фактор-множества $R(M_0,S_0)/\sim$, причем не существует двух или более вершин, помеченных одним и тем же элементом, а количество вершин ГП совпадает с числом элементов $R(M_0,S_0)/\sim$.

ГП для РСП РВ ТЛА всегда конечен, поскольку конечно множества $R(M_0,S_0)/\sim$:

- множество всех возможных маркировок M на конечном множестве мест сети конечно;
- максимальный возраст доступа каждого места задается в общем случае вещественным числом.

Анализ свойств сети может осуществляться с помощью маркировки узлов ГП и меток дуг. Каждая метка дуги представляет собой тройку, состоящую из перехода, его подстановки и значения временного промежутка перед его срабатыванием. Последний параметр позволяет определить время, затраченное на переход от одного состояния к другому. Используя алгоритмы поиска минимального и максимального пути между двумя узлами мультиграфа, можно найти минимальное и максимальное время перехода из одного состояния в другое. ГП позволяет увидеть все состояния сети с точностью до временных меток. Анализируя его, разработчик оценивает корректность выполнения поставленной задачи. Отметим, что ГП и для сравнительно малых РСП РВ ТЛА может достигать довольно больших размеров. Поэтому прямые исследования сетей путем их компьютерного моделирования могут упростить задачу разработчика.

2. Проверка правильности модели

2.1. Понятие верификации

Наиболее очевидным и широко распространенным методом проверки правильности программных систем является тестирование – проверка работы построенной системы в различных ситуациях, при различных исходных данных. Однако в случае с параллельными системами обычно невозможно заранее определить все возможные траектории функционирования. Поэтому в качестве основного метода повышения качества разработки применяется верификация – формальная проверка того, что система (модель) удовлетворяет сформулированным заранее требованиям [Карпов, 2010]. Методы верификации различаются в зависимости от того, какой аппарат лежит в основе проверяемой системы. Для верификации сложных систем свойства их поведения должны быть выражены формально логическими утверждениями, истинность которых зависит от времени, например, «Посланный запрос когда-нибудь позже будет обработан». Обычная логика высказываний является плохо пригодной для формулировки утверждений о поведении сложных динамических систем при изменении их состояний во времени. Формализация даже простейшего примера «Любой посланный запрос когда-нибудь позже будет обслужен» с помощью, например, логики предикатов первого порядка приводит к довольно громоздкому утверждению [Карпов, 2010]:

$$(\forall t \geq 0)\big(\ Послан(Запрос,t) \rightarrow$$
$$\rightarrow (\exists t' > t)(Обслужен(Запрос,t'))\ \big)$$

Поэтому при верификации темпоральных конструкций используются выражения темпоральных логик. Если нет необходимости подробно описывать закономерности поведения системы и взаимодействие ее объектов, целесообразнее применять не сложные интервальные логики, а простые расширения

обычной логики высказывания. Традиционно при верификации используются темпоральные логики линейного времени (*Linear Temporal Logic – LTL*) [Pnueli, 1977] и ветвящегося времени (*Computational Tree Logic – CTL*) [Clarce et al., 1986].

2.2. Метод верификации Model Checking

Перспективным методом верификации РСП РВ ТЛА является *Model Checking* (проверка модели) *MC* [Clarce et al., 1981]. Другие методы – дедуктивная верификация [Floyd, 1967] и проверка эквивалентности [Milner, 1980] – в общем случае не могут быть полностью автоматизированы, что негативно сказывается на возможности их применения при создании систем управления и ИСППР РВ. С другой стороны, исследования в области МС привели в последнее время к разработке очень эффективных алгоритмов верификации, позволяющих проверять реальные, разрабатываемые промышленностью программно-аппаратные системы. В частности, в работе [Карпов, 2010] приводятся эффективные алгоритмы *MC*, позволяющие проверить, что формула темпоральной логики *LTL* или *CTL*, выражающая некоторое свойство поведения динамической системы во времени, выполняется (является истинной) на модели системы с конечным числом состояний. В качестве модели при этом используется структура Крипке [Kripke, 1963], с помощью которой можно адекватно представить поведение реагирующих систем: дискретных систем управления, параллельных и распределенных алгоритмов, протоколов и т. п. Формально структура Крипке задается как пятерка

$$K = (W, W_0, H, AP, L), \text{ где:}$$

- W – конечное непустое множество состояний;
- $W_0 \subseteq W$ – непустое множество начальных состояний;
- $H \subseteq W \times W$ – множество переходов, удовлетворяющее требованию:

$$(\forall w \in W)(\exists w' \in W)((w, w') \in H);$$

- AP – конечное множество атомарных предикатов;
- $L : W \to 2^{AP}$ – функция пометок, сопоставляющая каждому состоянию множество истинных в нем атомарных предикатов.

Стандартными шагами доказательства того, что поведение реагирующей системы обладает некоторым свойством, являются следующие:

1) Для верифицируемой системы строится адекватная модель Крипке *K*, т. е. система переходов с конечным числом состояний. Поведения реальной системы представляются разверткой (деревом вычислений) построенной структуры Крипке.

2) С помощью переменных и параметров верифицируемой системы выражаются интересующие разработчика атомарные предикаты структуры Крипке – логические выражения, которые могут принимать значения «истина» или «ложь» в каждом состоянии системы.

3) Проверяемое свойство выражается формулой φ темпоральной логики *LTL* или *CTL* с использованием атомарных утверждений, темпоральных операторов и кванторов пути.

4) Проверяется истинность утверждения $K \models \varphi$ (т. е. утверждения, что структура Крипке является моделью формулы φ) с помощью полностью автоматизированной процедуры.

2.3. Верификация моделей РСП РВ ТЛА

Основную трудность при верификации по методу *MC* представляет необходимость построения структуры Крипке. Дальнейшие действия по проверке истинности темпоральных формул *LTL* или *CTL*, выражающих свойства системы, поддаются автоматизации, как показано в [Карпов, 2010]. В случае разработки модели процессов в парадигме формализма РСП РВ ТЛА нетрудно убедиться, что рассмотренный выше инструмент анализа ГП уже является структурой Крипке:

- *W* соответствует множество вершин ГП;
- W_0 соответствует вершина начального состояния (M_0,S_0);
- *H* соответствует множество переходов между вершинами ГП, требование существования перехода из любой вершины обеспечивается правилом построения ГП;
- *AP* соответствует конечное фактор-множество $R(M_0,S_0)/\sim$, содержащее по одному элементу для каждого класса эквивалентности по отношению покрытия состояний РСП РВ ТЛА;
- *L* соответствует функция пометок вершин ГП элементами множества $R(M_0,S_0)/\sim$

Таким образом, существует возможность автоматической верификации систем, разработанных на базе предложенного формализма; верификация РСП РВ ТЛА с помощью метода *MC* является естественным расширением начального анализа сетей с помощью графов состояний. Обобщенная схема процесса верификации приведена на рисунке 1.

Заключение

Общепризнано, что как тестирование, так и верификация по отдельности не могут гарантировать достаточного уровня правильности разрабатываемых систем. Существует большое число примеров, когда в тщательно проверенных и оттестированных реализациях с помощью верификации впоследствии обнаруживались тонкие ошибки. С другой стороны, нельзя надеяться только на верификацию. Часто причина ошибок кроется в том, что и при разработке, и при доказательстве алгоритмов неявно выдвигаются неправильные предположения о характере работы, т.е. используются неадекватные формальные модели.

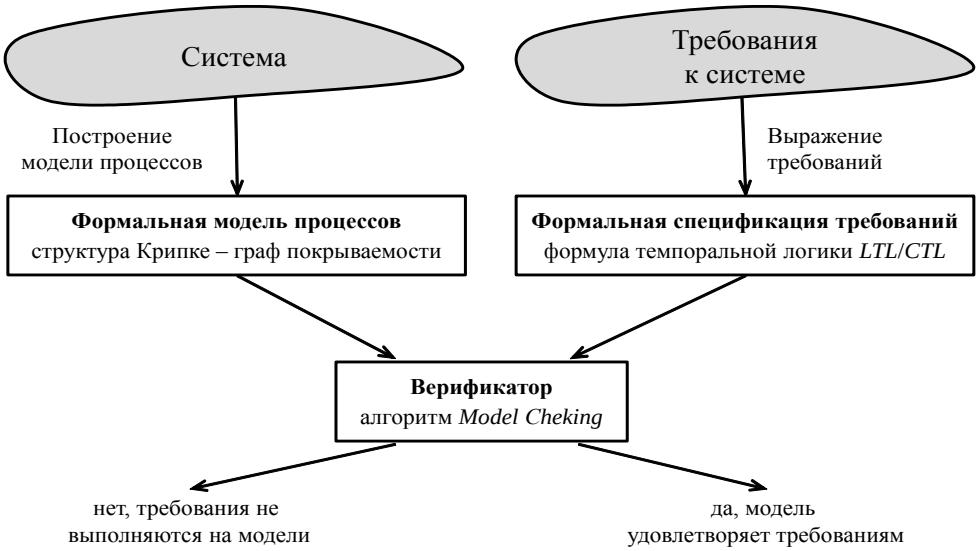

Рисунок 1 – Схема процесса верификации на основе алгоритма *Model Checking*

Таким образом, как тестирование, так и верификация обладают своими преимуществами и недостатками, поэтому эти подходы можно считать взаимодополняющими. Для повышения надежности реализаций при разработке систем управления, программных и аппаратных систем должны применяться оба подхода. В настоящий момент ведется разработка соответствующего программного обеспечения на языках высокого уровня, в которое планируется включить также возможность автоматической верификации моделей.

Библиографический список

[Вагин и др., 2001] Вагин В.Н., Еремеев А.П. Некоторые базовые принципы построения интеллектуальных систем поддержки принятия решений реального времени // Изв. РАН. Теория и системы управления. 2001. № 6. - С. 114-123.

[Осипов, 2008] Осипов Г.С. Динамические интеллектуальные системы // Искусственный интеллект и принятие решений. 2008. № 1. - С. 47-54.

[Еремеев и др., 2010] Еремеев А.П., Куриленко И.Е. Средства темпорального вывода для интеллектуальных систем реального времени // В кн.: Интеллектуальные системы. Коллективная монография. Выпуск 4./ Под. ред. В.М. Курейчика. - М.: Физматлит, 2010. - С. 222-252.

[Еремеев и др., 2013] Еремеев А.П., Королев Ю.И. Реализация интеллектуальных систем реального времени на основе сетей Петри с поддержкой темпоральных зависимостей // Программные продукты и системы. – 2013. – №3. – С. 88-94

[Еремеев и др., 2014] Еремеев А.П., Королев Ю.И. Анализ и верификация раскрашенных сетей Петри реального времени с поддержкой логики Аллена // Открытые семантические технологии проектирования интеллектуальных систем: материалы IV Междунар. научн.-техн. конф. (Минск, февраля 2014г.)/ редкол.: В.В. Голенков (отв. ред.) [и др.] – Минск: БГУИР, 2014. - С. 461-464.

[Карпов, 2010] Карпов Ю.Г. Model Cheking. Верификация параллельных и распределенных программных систем. – СПб.: БХВ-Петербург, 2010. – 560 с.

[Pnueli, 1977] Pnueli A. The temporal logic of program // Proc. of the 18th Anny. Symp. on Foundation of Computer Science. 1977. – P. 46-57.

[Clarce et al., 1986] Clarke E.M., Emerson E.A., and Sistla A.P. Automatic verification of finite-state concurrent systems using temporal logic specifications // ACM Trans. Program. Lang. Syst. 1986. Vol. 8. No. 2. – P. 244-263.

[Clarce et al., 1981] Clarke E.M., Emerson E.A. Design and synthesis of synchronization skeletons using branching-time temporal logic // Logic of Programs, 1981. - P. 52-71.

[Floyd, 1967] Floyd R.W. Assigning meaning to programs // Proc. Symposium on Applied Mathemtics. 1967. Vol. 9. - P. 19-32.

[Milner, 1980] Milner R. A Calculus of Communicating Systems. Lecture Notes in Computer Science, vol. 92. - Springer-Verlag, 1980.

[Kripke, 1963] Kripke S.A. Semantical consideration on modal logic // Acta Philosophica Fennica. 1963. Vol. 16. - P. 83-94.

VERIFICATION OF MODELS OF PROCESSES IN DYNAMIC SYSTEMS USING MODEL CHECKING METHOD

Eremeev A.P., Korolev Y.I.

National Research University «Moscow Power Engineering Institute», Moscow, Russia

Eremeev@appmat.ru

KorolevYu@gmail.com

In the paper the tools of modeling processes in complex dynamic systems are considered in terms of their use in intelligent decision support systems real time. A special type of Petri nets - real-time colored Petri net with support of Allen temporal logic is proposed to use as a basic formalism. The need to validate the models developed using this formalism is emphasized, it is proposed to use the Model Checking method of verification. This work was financially supported by RFBR and the Foundation for the promotion of innovation.

Keywords: intelligent decision support system, process modeling, Petri nets, temporal logic, system verification.