OSTIS-2014
(Open Semantic Technologies for Intelligent Systems)

УДК 007:519.816

АНАЛИЗ И ВЕРИФИКАЦИЯ РАСКРАШЕННЫХ СЕТЕЙ ПЕТРИ РЕАЛЬНОГО ВРЕМЕНИ С ПОДДЕРЖКОЙ ЛОГИКИ АЛЛЕНА

Еремеев А.П., Королев Ю.И.

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

Eremeev@appmat.ru

KorolevYu@gmail.com

Рассматриваются вопросы анализа темпорального подкласса сетей Петри, предложенного для моделирования интеллектуальных систем. Обуславливается необходимость верификации моделей, созданных на основе таких сетей. Предлагается использование графовых инструментов анализа, отражающих смену состояний в подобных сетях. Приводится пример построения таких графов для модели простой системы управления.
Работа выполнена при финансовой поддержке РФФИ (проект № 14-01-00427) и Фонда содействия инновациям.
Ключевые слова: модифицированные сети Петри; темпоральные модели; системы управления.

Введение

Проблема обеспечения правильности программных и аппаратных компонентов систем управления приобретает сегодня первостепенное значение. Надежность и предсказуемость поведения таких систем зачастую являются более важными свойствами, чем производительность, модифицируемость и т.п. На кафедре прикладной математики Национального исследовательского университета «Московский энергетический институт» (НИУ «МЭИ») уже более тридцати лет проводятся исследования по разработке математического и программного обеспечения интеллектуальных систем поддержки принятия решений (ИСППР) [Вагин, 1988]. При разработке таких систем, типичным представителем которых являются ИСППР реального времени (ИСППР РВ) для мониторинга и управления сложными техническими системами, используется предложенная Д.А. Поспеловым концепция семиотических систем управления [Поспелов, 1981] и аппарат нетрадиционных логик [Вагин и др., 2008]. В качестве одного из инструментов разработки предлагается использовать аппарат раскрашенных (цветных) сетей Петри реального времени с поддержкой логики Аллена (РСП РВ ЛА). Данный формализм позволяет корректно моделировать как количественные, так и качественные временные зависимости [Еремеев и др., 2013], упрощая процесс разработки моделей реальных систем. Однако использование сетей Петри подразумевает достаточно высокий уровень параллелизма, что, как и учет темпоральных зависимостей, может привести к возникновению ошибок и неточностей при разработке. Поэтому при применении аппарата РСП РВ с поддержкой логики Аллена актуален вопрос анализа и верификации моделей, созданных на его основе.

1. Повышение качества моделей

Параллельные, распределенные и 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 параллельной системы в целом, процессы в которой взаимозависимы. Такие системы, которые работают правильно «почти всегда», годами могут сохранять «тонкие» ошибки, проявляющиеся в исключительных ситуациях. Их непосредственными причинами являются и некорректные спецификации, и неправильное понимание спецификации разработчиками, несогласованность параллельных ветвей процессов и многое другое. 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. Рассматриваемый подкласс РСП РВ ЛА 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 процесса разработки, позволяют элегантно решить многие проблемы создания моделей систем (протекающих в них процессов), но зачастую делают целостное восприятие сложным. Поэтому для анализа поведения и верификации моделей, построенных с помощью РСП РВ ЛА, необходимо использовать дополнительные инструменты. Известны три основных группы методов анализа сетей Петри [Мурата, 1989]: основанные на построении графов изменения состояний; матричные методы, использующие уравнения сети и инварианты; методы редукции. При работе с раскрашенными и темпоральными сетями Петри последние две группы методов используются редко из-за высокой (по сравнению с классическими сетями Петри [Котов, 1984]) сложности формальных определений подобных подклассов. Чаще в качестве основного инструмента анализа рассматриваются графы достижимости и покрытия [Szpyrka, 2008].

2. Инструменты анализа

2.1. Смена состояний сети

Для работы с инструментальными средствами анализа РСП РВ ЛА, определим формально ключевые понятия состояния и перехода между состояниями. В качестве примера рассмотрим модель системы управления экстренным торможением поезда [Еремеев и др., 2013] (рисунок 1). Состояние сети представляет собой пару (M, S), где M - маркировка, функция на множестве мест P, а S - временной вектор, ставящий в соответствие каждому месту сети число - временную метку. Для сети, изображенной на рисунке 1, множество мест зададим следующим образом: P = {*Timer*1, *LightSig*, *SoundSig*, *Brake*, *Timer*2, *Driver*}. Тогда начальное состояние сети (M_0,S_0) будет выглядеть так:

$$\begin{aligned} M_0 &= (on, off, off, off, on, active), \\ S_0 &= (0, 0, 0, 0, 0, 0). \end{aligned} \quad (1)$$

Переход от одного состояния сети к другому может быть обусловлен двумя причинами:

- срабатыванием перехода $t \in T$ в подстановке b (подстановка - функция, которая замещает каждую переменную в защитной функции $G(t)$ и функциях весовых и временных значениях дуг E_M, E_S, влияющих на переход t, значением соответствующего типа);
- течением времени (постепенное уменьшение каждой временной метки на фиксированную величину, пока не появится переход, который может сработать).

Следует отметить, что безусловный приоритет при смене состояний сети имеет событие срабатывание перехода. Течение времени позволяет только дожидаться момента, когда может сработать очередной переход. Для рассматриваемого примера в начальном состоянии могут сработать два перехода: *TurnOnLS* и *Activity*. Рассмотрим изменение состояния сети при срабатывании первого. На переходе *TurnOnLS* защитная функция всегда принимает значение *true*, поэтому переход срабатывает в т.н. тривиальной подстановке b = (). Результатом срабатывания перехода *TurnOnLS* в начальном состоянии будет являться состояние (M_1,S_1):

$$\begin{aligned} M_1 &= (on, on, off, off, on, active), \\ S_1 &= (60, 0, 0, 0, 0, 0). \end{aligned} \quad (2)$$

При срабатывании перехода фишки-токены извлекаются и помещаются в места, связанные с переходом, в соответствии со значениями весовых выражений дуг, временные метки входных мест обнуляются, а временные метки выходных мест определяются в соответствии со значением временных выражений дуг, идущих из перехода к этим местам. В соответствии с условиями, накладываемыми защитной функцией, переход *Activity* может сработать в трех различных подстановках: $b_1 = (x/n)$, $b_2 = (y/n)$ и $b_3 = (z/n)$, где x $\in$ (0; 6), y $\in$ (6; 9), z > 9. Для удобства анализа примем x = 5, y = 8, z = 10. Результатом срабатывания перехода *Activity* в подстановке b_2 будет состояние (M_2,S_2):

$$\begin{aligned} M_2 &= (on, on, off, off, on, active), \\ S_2 &= (60, 0, 0, 0, 60, 8). \end{aligned} \quad (3)$$

Ни один переход не может сработать в этом состоянии. Необходимо подождать τ = 6 секунд, чтобы временная метка в месте *Console* позволила сработать переходу *TurnOnSS* (машинист не реагирует на световой сигнал):

$$S_2' = (54, -6, -6, -6, 54, 2). \quad (4)$$

После срабатывания перехода *TurnOnSS* в тривиальной подстановке сеть перейдет в новое состояние (M_3,S_3):

$$\begin{aligned} M_3 &= (on, on, on, off, on, active), \\ S_3 &= (54, 0, 0, -6, 54, 2). \end{aligned} \quad (5)$$

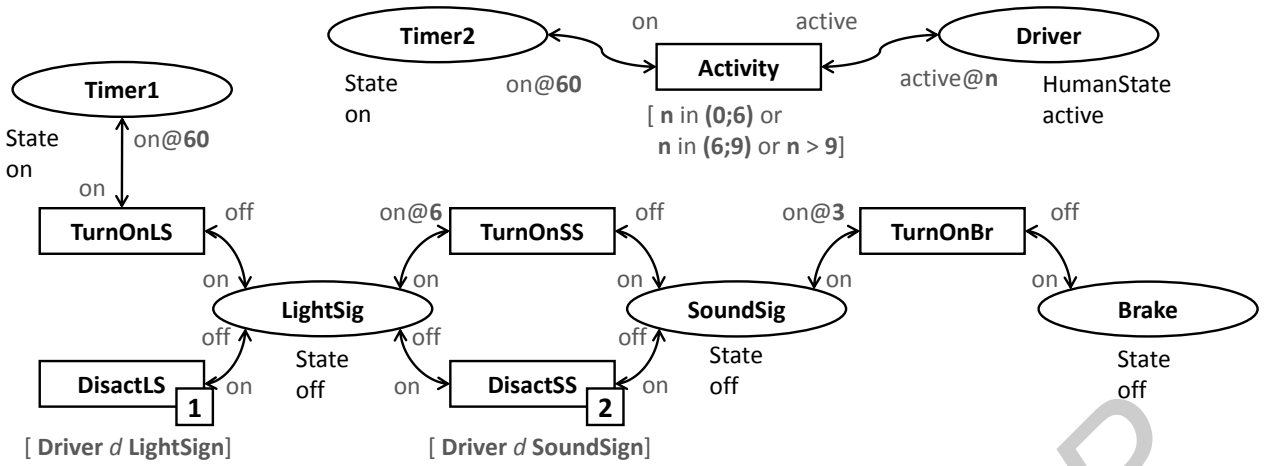

Рисунок 1 - Пример РСП РВ с поддержкой логики Аллена

Рассмотренную последовательность смены состояний сети (1-5) графически можно представить в следующем виде:

$$(M_0,S_0)\xrightarrow{(TurnOnLS(\ ))}(M_1,S_1)\rightarrow \xrightarrow{(Activity,(8/n))}(M_2,S_2)\xrightarrow{\tau=6}(M_2,S_2')\rightarrow \xrightarrow{(TurnOnSS(\ ))}(M_3,S_3)\longrightarrow\ldots \quad (6)$$

2.2. Граф достижимости

Будем считать, что состояние (M',S') достижимо из состояния (M,S), если существует конечная последовательность переходов, начинающаяся с состояния (M,S) и оканчивающаяся состоянием (M',S'). Обозначим за $R(M,S)$ множество всех состояний, достижимых из состояния (M,S). Анализ РСП РВ ЛА можно проводить, используя граф достижимости (ГД), вершинами которого являются элементы множества $R(M_0,S_0)$, а каждая дуга отображает изменение состояния (M_i,S_i) на (M_j,S_j) по прошествии времени $\tau \geq 0$ и срабатывания перехода t в подстановке b.

Граф, построенный по этим правилам для цепочки (6), представлен на рисунке 2.

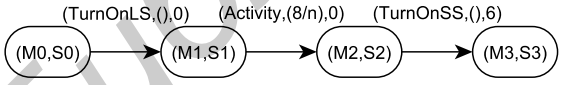

Рисунок 2 - Фрагмент графа достижимости

Анализ свойств сети может осуществляться с помощью маркировки узлов ГД и меток дуг. Каждая метка дуги представляет собой тройку, состоящую из перехода, его подстановки и значения временного промежутка перед его срабатыванием. Последний параметр, таким образом, позволяет определить время, затраченное на переход от одного состояния к другому. Используя стандартные алгоритмы поиска кратчайшего или длиннейшего пути между двумя узлами мультиграфа, можно найти минимальное и максимальное время перехода из одного состояния в другое.

Если продолжить строить ГД для анализируемой сети, можно убедиться, что из-за непрерывного уменьшения значений временных меток он оказывается бесконечным. Подобная ситуация возникает при анализе практически любой РСП РВ, в том числе, РСП РВ ЛА, причем степень связанности сети не влияет на конечность ГД. Очевидно, что в этом случае данный формализм неудобно использовать для анализа сетей. Введение дополнительных условий на временные метки позволяет трансформировать бесконечный граф в конечную структуру.

2.3. Граф покрытия

Одним из главных преимуществ РСП РВ ЛА является возможность представления множества достижимых состояний с помощью конечного графа покрытия (ГП). Отношение покрытия позволяет определять эквивалентные по своим характеристикам состояния сети Петри. Считаем, что два состояния покрывают друг друга, если их маркировки совпадают, а временные метки либо совпадают, либо не превышают максимального возраста доступа места $p \in P$, то есть такого значения временной метки, когда фишки-токены становятся доступными для всех выходных переходов места p.

Графы достижимости и покрытия строятся одинаково. Различие заключается только в способе добавления новой вершины в графы. Для 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. ГП содержит только одну вершину для каждого класса эквивалентности отношения покрытия состояний. ГП, построенный для анализируемой сети, приведен на рисунке 3.

ГП для РСП РВ ЛА предоставляет такие же возможности анализа сетевых свойств, как и

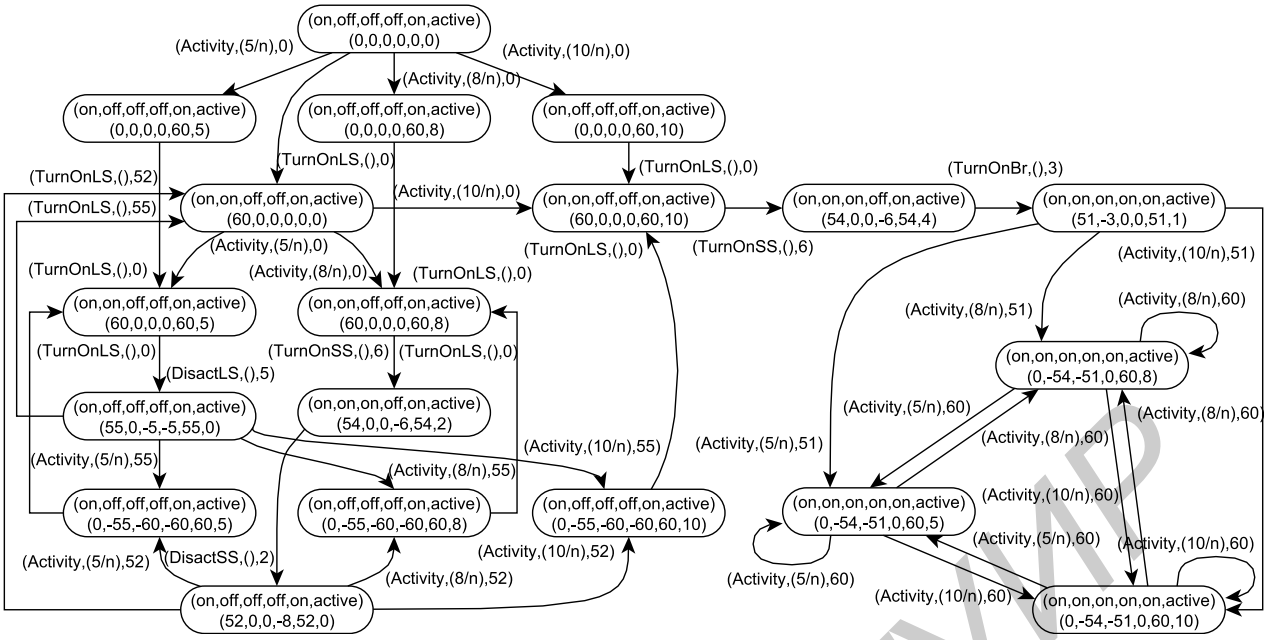

Рисунок 3 - Пример полного графа покрытия для РСП РВ с поддержкой логики Аллена

полный ГД. Он содержит все достижимые маркировки. Чтобы найти минимальное и максимальное время перехода из одного состояния в другое, можно использовать те же алгоритмы, что и для графов достижимости.

ГП сети позволяет увидеть все состояния с точностью до временных меток. Анализируя его, разработчик оценивает корректность выполнения поставленной задачи, т.е. верифицирует созданную модель. Отметим, что ГП и для сравнительно малых РСП РВ ЛА может достигать достаточно больших размеров. Поэтому прямые исследования сетей путем их компьютерного моделирования могут упростить задачу разработчика. Для проведения подобных исследований и разрабатывается базовый инструментарий [Еремеев и др., 2013].

Заключение

В работе рассматривается проблема анализа и верификации моделей, построенных на основе РСП РВ с поддержкой логики Аллена. В качестве основного инструмента анализа предложен модифицированный для РСП РВ граф покрытия.

Библиографический список

[Вагин, 1988] Вагин В.Н. Дедукция и обобщение в системах принятия решений. – М.: Наука, 1988. – 384 с.

[Вагин и др., 2008] Вагин В.Н., Головина Е.Ю., Загорянская Н.А., Фомина М.Б. Достоверный и правдоподобный вывод в интеллектуальных системах. –М.: Физматлит, 2008. – 712 с.

[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

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

[Котов, 1984] Котов В.Е. Сети Петри. – М.: Наука, 1984. – 160 с.

[Мурата, 1989] Мурата Т. Сети Петри: Свойства, анализ, приложения // ТИИЭР. - 1989. - т. 77, №4. - С. 41-85.

[Поспелов, 1981] Поспелов Д.А. Логико-лингвистические модели в системах управления. – М.: Энергоиздат, 1981. – 232 с.

[Szpyrka, 2008] Szpyrka M. Modelling and Analysis of Real-Time Systems with RTCP-Nets // Petri Net, Theory and Applications. I-Tech Education and Publishing. - 2008. – P. 17-40.

ANALYSIS AND VERIFICATION OF REAL-TIME COLORED PETRI NETS WITH SUPPORT OF ALLEN'S LOGIC

Eremeev A.P., Korolev Y.I.

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

Eremeev@appmat.ru

KorolevYu@gmail.com

In work analysis of temporal Petri nets' subclass, proposed by research group for intelligent systems' modeling, is considered.

Introduction

Formalism of real-time colored Petri nets with support of Allen's logic allows efficient simulation of the system, but the methods of analysis are needed to be defined to reduce the number of errors.

Main Part

Reachability graph is proposed to verify models. A set of places for such graphs is often infinite, as considered formalism is temporal. The concept of coverability is introduced. Coverability graph is proposed for models' analysis and verification.

Conclusion

Coverability graph modified for this type of network is proposed for models' analysis.