УДК 519.74, 681.51

Зайцев Д.А.
Zaitsev D.A.

СИНТЕЗ МОДЕЛЕЙ ПЕТРИ ТЕЛЕКОММУНИКАЦИОННЫХ ПРОТОКОЛОВ

SYNTHESYS OF PETRI NET MODELS OF TELECOMMUNICATION PROTOCOLS

Аннотация. Представлена методология синтеза моделей Петри телекоммуникационных протоколов. Выполнен обзор стандартов телекоммуникационных протоколов. В качестве промежуточного языка спецификаций использованы взаимодействующие последовательные процессы Хоара. Построены методы синтеза конечных автоматов по формуле последовательных процессов и синтеза помеченной сети Петри по формуле взаимодействующих последовательных процессов. Формализована задача синтеза непомеченной сети Петри заданной конечным автоматом.

Summary. A technique for Petri net models of telecommunication protocols synthesis was presented. A survey of telecommunication protocols' standards was implemented. As an intermediate language of specifications Hoare's communicating sequential processes were used. The methods of finite automata synthesis on formulae of sequential processes and methods of labeled Petri net synthesis on formulae of communicating sequential processes were developed. The task of unlabeled Petri net synthesis given by finite automata was formalized.

Сложность телекоммуникационных систем в настоящее время в значительной степени определяется сложностью протоколов [1], которые они реализуют. Протокол представляет собой набор правил, в соответствии с которыми взаимодействуют системы. При разработке телекоммуникационных систем протокол реализуется аппаратно либо программно. Спецификации протоколов представлены в стандартах, которые являются наиболее критичной информацией при разработке систем и должны быть корректными и обеспечивать эффективное взаимодействие. Процесс разработки протоколов становится всё более динамичным, так, например, количество известных протоколов удваивается каждые пять лет. Кроме того, возрастает сложность самих протоколов, что косвенно подтверждается ростом объема их стандартных спецификаций. Современный мир становится всё более зависимым от надёжности коммуникаций, что связано с увеличением количества передаваемой информации и повышением её значимости для общества. Электронная коммерция, технологическое управление предъявляют высокие требования к надёжности коммуникаций. Таким образом, формальное доказательство корректности телекоммуникационных протоколов представляет собой важную научную проблему.

Сети Петри [2] являются широко используемым средством верификации телекоммуникационных протоколов [3,4], а расширенные сети Петри [5,6] позволяют исследовать эффективность протоколов. Большинство стандартов используют подмножество естественного языка для спецификации протоколов, дополненного диаграммами, таблицами, схемами. Как правило, такие диаграммы состояний и схемы являются представлениями конечных автоматов. В условиях усложнения спецификаций и роста их объема становится актуальной задача автоматизации синтеза моделей Петри по исходным спецификациям. Методы, представленные в [7] позволяют выполнить верификацию моделей большого масштаба. Однако трудоёмкость верификации всё более обуславливается трудоёмкостью построения моделей, имеющей объёмы порядка тысяч элементов сети Петри.

Целью настоящей работы является создание эффективных методов синтеза моделей Петри с использованием промежуточного языка спецификаций, разработанного Чарльзом Хоаром – языка взаимодействующих последовательных процессов [8].

1. Стандарты телекоммуникационных протоколов. В настоящее время предпочтительным является применение широко известных протоколов по сравнению со специальными фирменными протоколами. Такой подход обеспечивает с одной стороны совместимость средств телекоммуникаций; кроме того, широко известные протоколы проходят процесс публичной верификации, в котором участвуют тысячи организаций и отдельных исследователей, что повышает их надёжность.

Ведущими организациями, обеспечивающих разработку и сопровождение протоколов в настоящее время являются: ISO (International Organization for Standardization – Международная организация по стандартизации, www.iso.org) выполняющая в основном методологические функции; IETF (Internet Engineering Task Force – Оперативная группа разработчиков Интернет, www.ietf.org), издающая RFC (References for comments – Справочники пояснений), специфицирующие протоколы применяемые в Интернет; IEEE (Institute of Electrical and Electronics Engineers – Институт инженеров электротехники и электроники, www.ieee.org), разрабатывающий в основном протоколы транспортного уровня; ITU (International Telecommunication Union – Международный союз телекоммуникаций, www.itu.int) специфицирующий протоколы физического уровня. Кроме того, известен целый ряд специальных групп SIG (Special Interest Group – Специальная группа интересов), обеспечивающих разработку и сопровождение отдельных протоколов либо их семейств. В такие группы входят представители известных компаний производителей аппаратных средств и программного обеспечения для телекоммуникаций, а также представители университетов и исследовательских организаций. Например, SIG Bluetooth (www.bluetooth.org) занимается сопровождением протокола Bluetooth мобильных сенсорных сетей. Имеется также большое число протоколов, разработанных отдельными компаниями. Как правило, такие протоколы вначале используются только фирмами производителями, а затем приобретают статус мировых стандартов. Одной из наиболее известных фирм, выполняющей разработку собственных протоколов является фирма CISCO, а в качестве примера известного стандарта можно указать протокол TACACS.

ISO представляет собой универсальную организацию, занимающуюся стандартизацией в различных областях деятельности человека. Хотя известен ряд конкретных телекоммуникационных протоколов, разработанных ISO, они не нашли широкого практического применения. Наибольшую известность получила эталонная модель взаимодействия открытых систем OSI.

IETF разрабатывает и сопровождает протоколы, которые находят наиболее широкое практическое применение в современном мире. Перечень официальных протоколов IETF, представленный в RFC 3600 в 2003 году насчитывает 214 протоколов. IETF определяет язык спецификаций в RFC 825, 1111 в документах Request for comments on Request for Comments: Instructions to RFC authors (Инструкции для авторов RFC). Документ содержит требование к формату текстовой информации, заголовкам, порядку описания. Процесс стандартизации описан в RFC 2026.

IEEE имеет в своей структуре специальное подразделение Standards Association (SA) – Ассоциация стандартов, которое занимается разработкой протоколов. Наиболее известными в настоящее время являются протоколы семейства Ethernet IEEE 802.3, а также протоколы беспроводных сетей IEEE 802.11. Для разработчиков стандартов IEEE-SA предлагает такие документы как IEEE Standards Association Operations Manual (Руководство к действию) и IEEE Standards Style Manual (Руководство по стилю стандартов).

Сектор ITU, разрабатывающий стандарты телекоммуникационных протоколов, носит название Telecommunication Standardization (Стандартизация телекоммуникаций) и обозначается как ITU-T. Он выпускает документы под названием ITU-T Recommendations (Рекомендации). Для разработчиков стандартов предлагается документ Author's Guide for drafting ITU-T Recommendations (Руководство для авторов рекомендаций).

Особый интерес представляет собой язык стандартных спецификаций протоколов, описывающий исходную информацию для разработчиков телекоммуникационных систем. Как правило, это подмножество естественного английского языка, дополненное специаль-

ными правилами спецификации стандартов, обеспечивающими сравнительную точность формулировок. Кроме того, для дополнительных уточнений применяют таблицы и диаграммы состояний, позволяющие уточнить вербальные спецификации. Известен также ряд специальных языков спецификации [1] для семейств протоколов, таких как CAPSL, HLPS, SMURPH, JXTA, но они не нашли широкого применения в действующих стандартах.

Стандартная спецификация протокола описывает порядок взаимодействия систем и форматы передаваемых сообщений (сигналов). Дополнительные требования могут включать временные параметры. Для описания структуры передаваемых сообщений в настоящее время широко используются языки, имеющие XML нотацию.

2. Взаимодействующие последовательные процессы как средство спецификации протоколов. Концепция взаимодействующих последовательных процессов (ВПП) была предложена выдающимся специалистом в области теории систем, лауреатом премии Тьюринга Чарльзом Энтони Ричардом Хоаром [8] в качестве универсального языка спецификации систем. ВПП представляют собой удобное средство, позволяющее перейти от естестественноязыковых спецификаций к формализованным и содержат минимально возможное количество используемых операций. Существенным ограничением формализма ВПП является абстрагирование от временных характеристик и рассмотрение лишь последовательностей событий. Такая абстракция вполне соответствует классическим сетям Петри, также абстрагирующимся от концепции времени. Вопросы эффективности протоколов требуют детального анализа временных характеристик и применения расширенных сетей Петри [5,6]. Таким образом, основная область применения ВПП – исследование корректности процессов, либо, применительно к протоколам, их верификация.

ВПП предназначены для описания поведения *объектов*. Поведение объектов формулируется в терминах *событий*. Событие является элементарным с точки зрения исследователя моментальным действием и полностью характеризуется своим *именем*. Множество всех допустимых событий формирует *алфавит* объекта. Следует отметить, что действия, имеющие некоторую временную протяжённость можно описывать парой событий, соответствующих началу и завершению действия. Термин *процесс* обозначает поведение объекта, представленное последовательностью происходящих событий. Алфавит процесса P обозначают αP.

Последовательный процесс описывается с помощью трёх основных операций:

1) Следование (префикс).

2) Рекурсия (итерация).

3) Выбор (альтернатива).

Пусть x – событие, а P – процесс. Тогда операция следования обозначается как $(x \to P)$ и описывает объект, который вначале участвует в событии x, а затем ведёт себя как процесс P. Например, пусть $\alpha P_1 = \{sendM, receivA\}$, где событие $sendM$ представляет собой отправку сообщения, а событие $receivA$ представляет получение подтверждения. Тогда процесс $P = (sendM \to Q)$ описывает процесс P, который отправляет сообщение, а затем ведёт себя как процесс Q.

Префиксную запись можно использовать для описания процесса, который после выполнения определённой последовательности событий остановится. Для описания поведения объектов, которые повторяют определенные последовательности действий, используется рекурсия. Для обозначения рекурсии имя определяемого процесса включают в его описание. Например, рекурсивное определение $P_1 = (sendM \to (receivA \to P_1))$ описывает процесс P_1, который отправляет сообщение, получает подтверждение, а затем ведёт себя точно так же, как процесс P_1, то есть выполняет указанную последовательность неограниченное число раз.

Выбор используют для описания альтернатив в поведении объекта. Пусть x, y – различные события; тогда формула $(x \to P | y \to Q)$ описывает объект, который сначала участвует в одном из событий x либо y, а затем ведёт себя как P, если произошло событие x либо как

процесс Q, если произошло событие y. Например, дополним алфавит объекта P_1 событием $fault$, соответствующим его поломке $\alpha P_1' = \{sendM, receivA, fault\}$, тогда процесс $P_1' = (sendM \to (receiveA \to P_1 \,|\, fault \to stop))$ описывает объект, который может сломаться после получения подтверждения. Заметим, что более точным является описание объекта, который может сломаться также и после отправки сообщения $P_1'' = (sendM \to (receiveA \to P_1 \,|\, fault \to stop) \,|\, fault \to stop)$.

В качестве *протокола поведения процесса* Хоар рассматривает конечную последовательность символов, фиксирующих события, в которых процесс участвует до некоторого момента времени. *Спецификацией* названо описание предполагаемого (идеального) поведения. Именно термин спецификация соответствует термину протокол, используемому в области телекоммуникаций. Стандарты телекоммуникационных протоколов представляют собой множество их спецификаций на естественном языке.

Существенным для описания телекоммуникационных систем является представление параллельных процессов в терминах взаимодействующих последовательных процессов. Для представления взаимодействия Хоаром использована операция параллельной композиции процессов: $P \,||\, Q$ обозначает процесс, ведущий себя как система, в которой события объектов P и Q чередуются в произвольном порядке, если они имеют разные имена и требуют синхронизации, если имена событий совпадают. Таким образом, если событие входит в алфавиты двух объектов, то для его возникновения необходимо, чтобы оно стало возможным для обоих процессов.

Дополненные операцией параллельной композиции, ранее введенные операции следования, рекурсии и выбора, представляют собой минимальное множество операций, используемых Хоаром для описания произвольных процессов. Указанное множество операций дополняется в монографии [8] рядом вспомогательных операций и функций, обеспечивающих компактность описаний сложных объектов, кроме того, разрабатываются алгебраические методы доказательства корректности процессов. Следует отметить некоторую громоздкость дополнительных конструкций; кроме того, особенностью методов доказательства корректности является их организация в виде правил вывода, не гарантирующих доказательство корректности произвольного процесса. Таким образом, использование ВПП оправдано в качестве промежуточного языка при переходе от естественноязыковых спецификаций к моделям Петри.

Рассмотрим пример построения ВПП простейшего телекоммуникационного протокола, задающего одностороннюю передачу сообщений с подтверждениями:

Передающая подсистема: $P_1 = (sendM \to (receivA \to P_1))$.

Принимающая подсистема: $P_2 = (receivM \to (sendA \to P_1))$.

Канал передачи сообщений: $P_M = (sendM \to (receivM \to P_M))$.

Канал передачи подтверждений: $P_A = (sendA \to (receivA \to P_A))$.

Телекоммуникационный протокол: $S = P_1 \,||\, P_2 \,||\, P_M \,||\, P_A$.

В системе, функционирующей в соответствии с S, допустима единственная последовательность событий вида $sendM$, $receivM$, $sendA$, $receivA$,...

3. Модели Петри взаимодействующих последовательных процессов. Модели Петри представляют собой простой и мощный формализм для представления и верификации параллельных процессов [2-6]. Напомним, что сеть Петри [2] $N = (P, T, F, \mu_0)$ является двудольным ориентированным графом, дополненным динамическими элементами – фишками; $P = \{p\}$ – множество вершин, называемых позициями, $T = \{t\}$ – множество вершин, называемых переходами, кроме того $P \cap T = \varnothing$, потоковая функция $F : (P \times T) \cup (T \cup P) \to \mathrm{N}$ задаёт дуги сети и их кратность, где N – множество целых неотрицательных чисел, начальное распреде-

ление фишек по позициям задано начальной маркировкой $\mu_0 : P \to \mathrm{N}$. Фишки перемещаются по сети в результате срабатывания переходов [2].

Выбор сетей Петри для верификации протоколов обусловлен широким набором известных методов их анализа [2-6], а также компьютерных моделирующих систем, обеспечивающих автоматизацию процессов верификации. Применение методов теории функциональных сетей Петри [7] позволяет выполнять анализ крупномасштабных моделей за приемлемое время. Следует отметить, что именно большая размерность детализированных моделей телекоммуникационных протоколов сдерживала широкое применение методов сетей Петри для верификации протоколов. Целью настоящего раздела является построение методов синтеза сети Петри заданной формулой ВПП.

Заметим, что последовательный процесс может быть представлен конечным автоматом Мили, входной алфавит которого пуст, а выходной алфавит задан алфавитом событий процесса. Состояниями автомата являются символы процессов в формуле ВПП, а также промежуточные символы, соответствующие операциям следования.

Правила построения конечного автомата A_P по формуле последовательного процесса P:

1) $A_P = (X, Q, Y, q_0, F)$, где $X = \varnothing$ – входной алфавит, $Y = \alpha P$ – выходной алфавит, Q – конечное множество внутренних состояний, $q_0 = P$ – начальное состояние, $F: Q \to Y \times Q$ – функция переходов.

2) Состояния автомата. Разобьем формулу P на эквивалентное множество формул с помощью вспомогательных переменных-процессов P_i следующим образом: если в некоторой операции следования $x \to R$, правая часть R представляет собой формулу (не символ процесса), то заменим формулу R новым символом состояния автомата P_i и продолжим преобразования над формулой $P_i = R$.

3) Функция переходов. Для каждой формулы вида $P_i = y \to P_j$ добавим переход из состояния P_i в состояние P_j, с выходным сигналом y.

Например, для протокола S имеем:

$P_1 = (sendM \to P_{1,1})$, $P_{1,1} = (receivA \to P_1)$;

$P_2 = (receivM \to P_{2,1})$, $P_{2,1} = (sendA \to P_1)$;

$P_M = (sendM \to P_{M,1})$, $P_{M,1} = (receivM \to P_M)$;

$P_A = (sendA \to P_{A,1})$, $P_{A,1} = (receivA \to P_A)$.

Соответствующее множество автоматов представлено на Рис. 1.

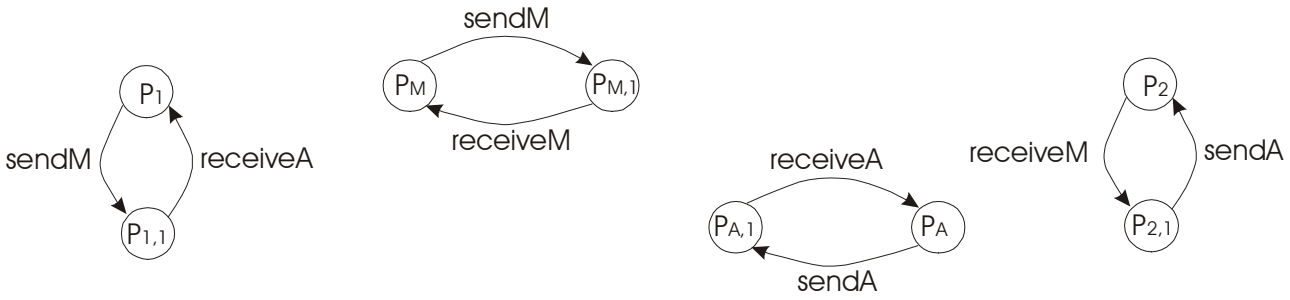

Рисунок 1 – Конечные автоматы последовательных процессов P_1, P_2, P_M, P_A

Теорема 1. Построенный конечный автомат A_P является представлением процесса P.

Доказательство. Применение правила 2) обеспечивает построение множества формул вида

$$P_i = x_1 \to P_{i,1} \mid x_2 \to P_{i,2} \mid \ldots \mid x_l \to P_{i,l}$$

эквивалентного исходной формуле процесса P. Применение правила 3) обеспечивает построение функции переходов автомата, содержащей переход $q_{P_i} \to (x_j, q_{P_{i,j}})$ для каждой формулы $P_i = x \to P_{i,j}$ и не содержащей никаких других переходов. ■

Заметим, что после построения конечного автомата может быть выполнена его минимизация с помощью известных алгоритмов [9,10]. Следует также отметить, что аналогичным образом можно определить автомат с входным алфавитом, совпадающим с алфавитом процесса, и пустым выходным алфавитом; такой автомат можно рассматривать как распознаватель корректных последовательных процессов.

Построим помеченную автоматную сеть Петри APN_P как указано в [2], заменяя каждое состояние автомата позицией сети Петри, а каждую дугу автомата, помеченную символом y последовательностью из дуги, перехода, помеченного символом y и дуги; поместим единственную фишку в позицию, соответствующую начальному состоянию. Представления процессов P_1, P_2, P_M, P_A помеченными автоматными сетями Петри изображены на Рис. 2.

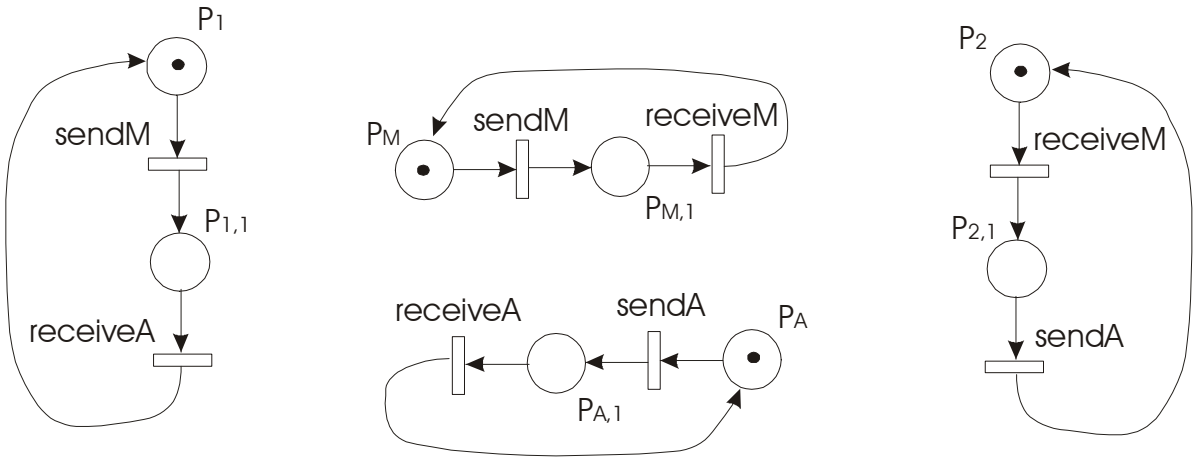

Рисунок 2 – Автоматные сети Петри процессов P_1, P_2, P_M, P_A

Утверждение. Автоматная помеченная сеть Пери APN_P является представлением процесса P.

Построим представление параллельной композиции для сетей Петри. Пусть автоматные помеченные сети Петри APN_{P_1}, APN_{P_2} являются представлениями последовательных процессов P_1 и P_2 соответственно. Построим сеть Петри APN_P следующим образом: объединим каждый из переходов сети APN_{P_1} с каждым из переходов сети APN_{P_2}, помеченные одинаковым символом события y. Пример построенной модели телекоммуникационного протокола S представлен на Рис. 3.

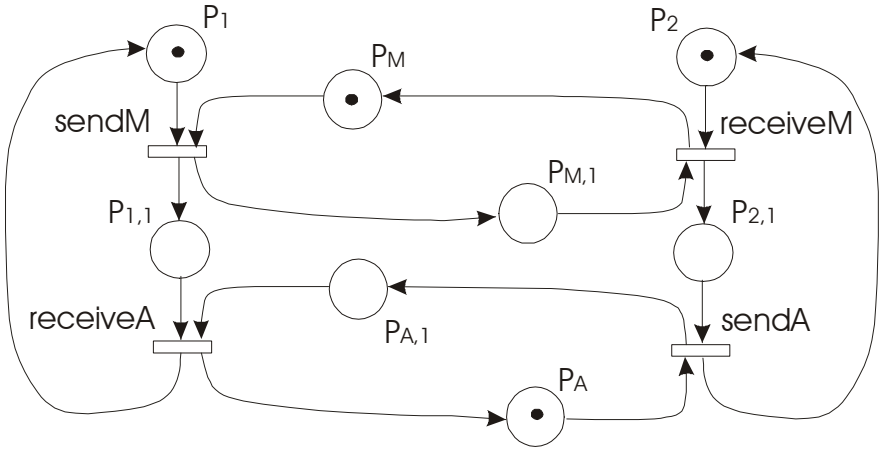

Рисунок 3 – Модель телекоммуникационного протокола S

Теорема 2. Сеть Петри APN_P является представлением формулы $P = P_1 \| P_2$.

Доказательство. Так как каждая из сетей APN_{P_1}, APN_{P_2} имеет фишку в своей начальной маркировке, поведение сети APN_P представляет собой произвольное чередование событий процессов P_1 и P_2 до тех пор, пока не появятся условия возбуждения перехода, соответствующего событию, принадлежащему алфавитам обоих процессов. Правила срабатывания перехода сети Петри требуют наличия фишек во входных позициях двух процессов одновременно. После срабатывания перехода фишки появятся в выходных позициях двух процессов, что обеспечивает их дальнейшее независимое выполнение. Таким образом, поведение сети APN_P соответствует определению операции параллельной композиции процессов Хоара. ■

Следствие. Сети Петри с помеченными переходами эквивалентны ВПП.

4. Синтез сети Петри заданной конечным автоматом. Следует отметить, что автоматная сеть Петри с помеченными переходами является наиболее простым, но не единственным способом представления конечного автомата. В такой сети множества переходов могут иметь одинаковую пометку события y. В настоящем разделе формализована задача синтеза классической сети Пери (без помеченных переходов), эквивалентной заданному конечному автомату. В такой сети каждое событие y представлено единственным переходом t_y. Задача может быть сформулирована как оптимизационная с целевой функцией, минимизирующей количество элементов (позиций, дуг) сети Петри.

Пусть состояния автомата q_i, $i = \overline{0, k-1}$ закодированы маркировками сети $\bar{\mu}_i$, а переходы сети t_y соответствуют событиям $y \in Y$ и представлены парой векторов $\bar{t}_y^-$ и $\bar{t}_y^+$, задающими входящие и исходящие дуги перехода соответственно. Тогда, с одной стороны, необходимо, чтобы каждый переход t_y, соответствующий событию $y \in Y$, представленному дугой автомата $q_i \xrightarrow{y} q_j$, был разрешен в маркировке $\bar{\mu}_i$, и его срабатывание приводило к маркировке $\bar{\mu}_j$. А с другой стороны, необходимо, что все остальные переходы t_z, события которых невозможны в состоянии q_i были запрещены в маркировке $\bar{\mu}_i$. Имеем:

$$\begin{cases} \bar{\mu}_i \geq \bar{t}^-, \ \ \forall t \in T_y, \\ \bar{\mu}_j - \bar{\mu}_i - \bar{t}^- + \bar{t}^+ = 0, \ \ \forall t \in T_y, \\ \neg(\bar{\mu}_i \geq \bar{t}^-), \ \ \forall t \notin T_y, \\ T_y = \{t \,|\, q_i \xrightarrow{y} q_j\}, \forall y \in Y. \end{cases} \tag{1}$$

Теорема 3. Сеть Петри, удовлетворяющая системе (1) является представлением конечного автомата A_P.

Доказательство. По построению каждый переход сети является представлением выходного символа автомата, а каждая допустимая маркировка – представлением состояния автомата. Для каждой пары состояний q_i, q_j такой, что $\exists y \in Y$: $q_i \xrightarrow{y} q_j$ первый и второй термы системы (1) обеспечивают, что сеть Петри в соответствии с уравнением состояний [2] перейдёт из маркировки $\bar{\mu}_i$ в маркировку $\bar{\mu}_j$ в результате срабатывания перехода t_y. Кроме того, третий терм обеспечивает, что никакой другой переход t_z не сработает в маркировке $\bar{\mu}_i$. ■

Следует отметить, что система (1) содержит алгебраические уравнения и неравенства, а также логические операции. Необходима разработка специальных методов эффективного решения таких систем. Кроме того, размерность векторов, соответствующая количеству позиций сети заранее неизвестна. Пусть количество позиций сети Петри равно m. Тогда задача синтеза сети Петри с минимальным количеством позиций может быть представлена целевой функцией (2), а задача синтеза сети Петри с минимальным количеством дуг (учитывая их кратность) – целевой функцией (3).

$$m \to \min, \tag{2}$$

$$\sum_{y \in Y} \sum_{j=i.m} t^-_{y,j} + \sum_{y \in Y} \sum_{j=i.m} t^+_{y,j} \to \min. \tag{3}$$

В заключение следует отметить, что в настоящей работе построены методы синтеза конечных автоматов по формуле последовательных процессов и синтеза помеченной сети Петри по формуле взаимодействующих последовательных процессов, а также формализована задача синтеза непомеченной сети Петри заданной конечным автоматом.

Разработанные методы предназначены для автоматизации процессов построения моделей Петри по стандартным спецификациям телекоммуникационных протоколов. В качестве промежуточного языка спецификаций использованы взаимодействующие последовательные процессы Хоара.

Литература

1. Russell T. Telecommunications Protocols, 2nd Edition, McGraw-Hill, 2004.
2. Мурата Т. Сети Петри: Свойства, анализ, приложения // ТИИЭР, т. 77, №4, 1989, с. 41-85.
3. Girault C., Volk R. Petri nets for systems engineering – A guide to modelling, verification and applications. Springer-Verlag, 2003.
4. Cortadella J., Kishinevsky M., Kondratyev A., Lavagno L., Yakovlev A. Logic synthesis of asynchronous controllers and interfaces. Springer-Verlag, 2002.
5. Слепцов А.И., Юрасов А.А. Автоматизация проектирования управляющих систем гибких автоматизированных производств / Под ред. Б.Н.Малиновского. К.: Техніка, 1986, 160 с.
6. Jensen K. Colored Petri Nets – Basic Concepts, Analysis Methods and Practical Use.- Vol. 1-3, Springer-Verlag, 1997.
7. Zaitsev D.A. Functional Petri Nets, Universite Paris-Dauphine, Cahier du Lamsade 224, Avril 2005, 62p (www.lamsade.dauphine.fr/cahiers.html).
8. Хоар Ч. Взаимодействующие последовательные процессы. М.: Мир, 1989, 264с.
9. Глушков В.М. Синтез цифровых автоматов. М.: Физматгиз, 1962.- 476с.
10. Ахо А., Ульман Дж. Теория синтаксического анализа, перевода и компиляции. Т.1: Синтаксический анализ. М.: Мир, 1978, 488с.