Российская академия наук
Сибирское отделение
Институт систем информатики
им. А.П.Ершова

На правах рукописи

Окунишникова Елена Валерьевна

МОДЕЛИРОВАНИЕ ESTELLE-СПЕЦИФИКАЦИЙ РАСПРЕДЕЛЕННЫХ СИСТЕМ С ПОМОЩЬЮ РАСКРАШЕННЫХ СЕТЕЙ ПЕТРИ

05.13.11 — математическое и программное обеспечение
вычислительных машин, комплексов и компьютерных сетей

Автореферат
диссертации на соискание ученой степени
кандидата физико-математических наук

Новосибирск, 2004

Работа выполнена в Институте систем информатики
Сибирского отделения Российской академии наук

Научный руководитель:	кандидат физико-математических наук Непомнящий В.А.
Официальные оппоненты:	доктор физико-математических наук Ломазова И.А. кандидат физико-математических наук Скопин И.Н.
Ведущая организация:	Ярославский государственный университет (г. Ярославль)

Защита состоится 14 сентября 2004 года в 15 час. 00 мин. на заседании диссертационного совета К003.032.01 в Институте систем информатики им А. П. Ершова Сибирского отделения РАН по адресу:

630090, г.Новосибирск, пр. Лаврентьева, 6.

С диссертацией можно ознакомиться в читальном зале библиотеки ИСИ СО РАН (пр. Лаврентьева, 6).

Автореферат разослан "_____" августа 2004 г.

Ученый секретарь
диссертационного совета
К003.032.01
к.ф.-м.н. Мурзин Ф.А.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность. Сложность и многообразие функций, выполняемых современными информационно-вычислительными сетями, привели к разработке многочисленных формальных моделей, используемых в настоящий момент для спецификации распределенных систем. При этом возрастающая потребность в распределенных вычислительных системах и сетях ЭВМ требует не только реализации таких систем на основании формальных описаний, но и повышения эффективности методов проектирования путем создания инструментальных средств, предназначенных для автоматизации процессов проектирования и анализа.

Распространение сетей Петри и их различных модификаций в качестве модели, используемой для спецификации распределенных систем, обусловлено тем, что они сочетают строгую, хорошо проработанную формальную теорию с наглядным графическим представлением. Систематическое изучение свойств сетей Петри началось на рубеже 60-х и 70-х годов и продолжается по сей день. Среди отечественных авторов, в разное время занимавшихся исследованиями в области сетей Петри, можно отметить Н.А.Анисимова, О.Л.Бандман, И.Б.Вирбицкайте, В.Е.Котова, И.А.Ломазову, В.А.Соколова, Л.А.Черкасову и многих других. Раскрашенные сети Петри (РСП), предложенные К.Йенсеном, получили широкое признание как удобный, мощный и эффективный механизм для спецификации и верификации свойств распределенных систем, что подтверждается ведущимися работами по принятию РСП в качестве стандарта ISO.

С другой стороны, на практике используются языки выполнимых спецификаций, "лидерами" среди которых являются языки Estelle (стандарт ISO) и SDL (стандарт ITU). Языки выполнимых спецификаций имеют формальный базис, а их близость к языкам программирования облегчает процесс последующей реализации. Однако способы анализа выполнимых спецификаций остаются предметом исследования. Поэтому широко используется практика отображения спецификаций в формальные модели, для которых существуют эффективные методы анализа и автоматические средства верификации. Известны примеры транс-

ляции выполнимых спецификаций в конечно-автоматные модели, сети Петри, алгебры процессов и темпоральные логики действий.

Опубликован ряд работ по трансляции SDL-спецификаций в различные классы сетей Петри, среди которых можно выделить два направления. Первое использует известные классы сетей Петри высокого уровня, такие как PrT-сети (работы Е. Кеттунена и Н. Хусберга) и M-сети (работы Б.Гралмана). Для второго характерно создание новых классов сетей Петри, ориентированных на язык (работы Й.Фишера и Ф.Баузе).

Для Estelle-спецификаций в работе Ж.Л.Ричье, Й.Сифакиса и др. предложен метод автоматического построения конечно-автоматных моделей посредством исчерпывающей симуляции, позволяющий верифицировать некоторые свойства коммуникационных протоколов. В работах В. Димитрова ограниченное подмножество Estelle отображается в ординарные сети Петри. А. Яновская и П. Яновский предлагают способ перевода подмножества Estelle, не включающего динамических возможностей Estelle, времени и приоритетов, в темпоральную логику TLA+.

В работах Р. Лая и А. Джирачифпаттаны предложен метод отображения Estelle-спецификаций в нумерические сети Петри, который рассматривает подмножество языка, включающее динамические конструкции. Однако время и приоритеты не рассматриваются. Помимо этого, данный метод требует предварительной ручной обработки Estelle-спецификации. В более поздних работах Р. Лая и Т. Цанга для моделирования поведения, явно зависящего от времени, используются модульные сети Петри. Однако в этих работах авторы рассматривают не стандартный Estelle, а предлагают расширение языка, приближающее его к языкам реального времени. Кроме того, реализация предложенных методов упоминается только как тема для исследования. Моделирование выполняется отдельно для каждого примера, что приводит к необходимости верификации процесса моделирования.

Таким образом, автоматический перевод выполнимых спецификаций в формальные модели, для которых существуют эффективные методы анализа и автоматические средства верификации, представляет значительный интерес. В частности, в книге К.Йенсена поставлена проблема автоматического построения сетевых моделей SDL-спецификаций, развития средств их верификации, а также проведения экспери-

ментов по обнаружению семантических ошибок распределенных систем с помощью этих средств. Несомненна актуальность аналогичной проблемы и для Estelle-спецификаций.

Цель диссертации состоит в разработке эффективных методов и средств моделирования и валидации распределенных систем, представленных на языке Estelle.

Методы исследования базируются на применении аппарата сетей Петри и языка выполнимых спецификаций Estelle.

Научная новизна состоит в следующем.

• Разработан алгоритм перевода Estelle-спецификаций без динамических конструкций в раскрашенные сети Петри. Проведено моделирование представительного подмножества языка Estelle-спецификаций, включающего отложенные переходы и приоритеты. Для моделирования последних предложена расширенная модель раскрашенных сетей, включающая в себя временной механизм и приоритеты. На основании анализа сетевых моделей, получающихся в результате отображения статических Estelle-спецификаций, разработан вариант раскрашенных сетей — иерархические временные типизированные сети (ИВТ-сети), — одной из особенностей которого является отсутствие перебора вариантов связывания переменных, что позволяет существенно повысить эффективность моделирования при реализации.

Впервые предложено формальное обоснование алгоритма. Доказано, что сеть, моделирующая статические Estelle-спецификации, безопасна. Введено понятие эквивалентности состояния Estelle-модуля и разметки моделирующей его сети и показано, что выполнение Estelle-перехода сохраняет эквивалентность состояния и разметки. Дана оценка размера моделирующей сети.

• Разработан способ моделирования динамических средств Estelle и алгоритм перевода спецификаций с динамическими конструкциями в раскрашенные сети Петри. Впервые проведено моделирование, охватывающее практически полный язык Estelle, посредством раскрашенных сетей Петри, что позволяет решить проблему автоматического построения сетевых моделей Estelle-спецификаций.

Дано обоснование предложенного алгоритма. Введен аналог свойства безопасности — послойная безопасность. Показано, что сеть, мо-

делирующая динамические Estelle-спецификации, послойно безопасна. Расширено понятие эквивалентности состояния спецификации и разметки моделирующей сети. Доказано, что выполнение Estelle-перехода сохраняет эквивалентность состояния и разметки. Приведена оценка размера моделирующей сети.

Практическая ценность данных исследований заключается в их использовании при реализации трансляторов с языка Estelle в ИВТ-сети, а также в проведении экспериментов по валидации коммуникационных протоколов, в частности, кольцевого протокола. Автоматическое построение сетевых моделей существенно сокращает трудоемкость по проведению экспериментов и избавляет от необходимости проводить верификацию самого процесса построения, а поуровневое представление делает возможным построение сетевых моделей для систем реальной сложности. Предложенные алгоритм перевода и ИВТ-сети используются в системе EPV.

Апробация работы. Основные научные и практические результаты подробно обсуждались на объединенном семинаре ИСИ СО РАН и кафедры программирования НГУ "Теоретическое и экспериментальное программирование", докладывались на следующих научных конференциях:

1. *3rd International Conference on Parallel Computing Technologies,* St.Petersburg, Russia, 1995.
2. *IFIP 15th International Symposium on Protocol Specification, Testing and Verification,* Warsaw, Poland, 1995.
3. *Third International Workshop on Concurrency, Specification and Programming,* Warsaw, Poland, October 1997.
4. *15-th IMACS World Congress on Scientific Computation, Modelling and Appl.,* Berlin, Germany, 1997.
5. *International Conference on Parallel Computing in Electrical Engineering,* Bialystok, Poland, 1998.
6. *1st International Workshop on the Formal Description Technique Estelle,* Evry, France, 1998.
7. *Четвертый Сибирский Конгресс по Прикладной и Индустриальной Математике (ИНПРИМ-2000),* Новосибирск, Россия, 2000.
8. *Конференция молодых ученых, посвященная 10-летию ИВТ СО РАН,* Новосибирск, Россия, 2000.

Работа поддерживалась следующими грантами: РФФИ 93-01-986, 1993—1995; Международного Научного Фонда и Российского правительства, JCP 100, 1994; ИНТАС 1010-CT93-0042, 1993—1994; ИНТАС-РФФИ N 95-0378, 1997—1999; Президиума СО РАН Поддержки международных проектов, 1997.

Публикации. По теме диссертации опубликовано 16 научных работ.

Структура работы. Диссертация состоит из введения, четырех глав, заключения, списка литературы из 81 наименования и приложения. Объем основной части работы — 140 страниц, приложения — 7 страниц.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность диссертации и формулируются ее цели, характеризуется научная новизна и практическая ценность работы.

В **первой главе** дано описание языка формальных описаний Estelle и краткое напоминание основных понятий теории раскрашенных сетей, предложенных Йенсеном. Приставки E- и N- используются для обозначения объектов (модуля, перехода) Estelle и сети соответственно.

В **разд. 1.1** приводятся необходимые сведения о языке Estelle, основанном на объединении конечного автомата с языком программирования Pascal и добавлении элементов описания архитектуры системы, которая определяется иерархически организованным множеством модулей и структурой их взаимосвязей. Для взаимосвязи между модулями служат двунаправленные каналы между портами (*точками взаимодействия*).

В **разд. 1.2** дается определение раскрашенных сетей Петри. Каждая фишка в РСП обладает значением некоторого типа, которое называется *цветом*. Сеть включает в себя описание множеств цветов (типов), переменных и функций. С каждым местом связан тип, из которого могут принимать значения фишки в данном месте. Дуги помечаются выражениями. Переходы имеют спусковые функции. Функционирование РСП зависит не только от наличия фишек во входных местах переходов, но и от их цвета. Срабатывание перехода изымает по фишке из каждого входного места перехода и помещает по фишке в каждое

его выходное место. Значения фишек определяются выражениями на соответствующих дугах.

Иерархическая раскрашенная сеть — это композиция множества неиерархических сетей, называемых *страницами*. Страницы могут содержать вершины, которые называются *модулями* и графически представляют подсеть, располагающуюся на отдельной странице. Коммуникация между страницами происходит с помощью мест, связанных с модулями. Подстраница модуля содержит копии всех мест, с которыми он связан. Место-прототип и его копия являются образами одного и того же "концептуального" места и всегда имеют одинаковую разметку.

В **разд. 1.3** для РСП вводятся приоритеты и два временных механизма. Во временных сетях, предложеных Мерлином, каждому переходу приписывается интервал срабатывания $[d_{min}, d_{max}]$, где d_{min} определяет минимальное время, которое должно пройти до того момента, как возможный переход сработает, а d_{max} — максимальное время, в течение которого переход может оставаться возможным и не сработать. Второй механизм, предложенный Йенсеном, использует понятия глобальных часов и временных штампов фишек. Глобальные часы показывают текущее время в сети. Значение временного штампа определяет, когда фишка может быть использована: фишка остается недоступной для переходов, пока текущее время и значение ее временного штампа не станут равны. Временной штамп фишки может определяться как переходом, так и дугой, по которой фишка "поступила" в место.

Сети с приоритетами — это сети, в которых каждому переходу сопоставлено некоторое неотрицательное целое число. Возможный переход может сработать, если его приоритет не меньше приоритета любого другого возможного перехода.

Вторая глава посвящена алгоритму перевода подмножества Estelle в РСП, расширенные приоритетами и временным механизмом Мерлина. Рассматриваются спецификации, в которых не происходит динамического создания и уничтожения экземпляров модулей, не изменяется структура связей, а также не используются рекурсивные процедуры и функции.

В **разд. 2.1** рассматриваются правила преобразования предопределенных типов Estelle в множества цветов РСП.

В **разд. 2.2** описывается отображение иерархии модулей в дерево страниц РСП. Корнем является страница, на которой представлена общая структура спецификации. Отображение E-модуля происходит по одной схеме независимо от его положения в иерархии спецификации. Каждому экземпляру E-модуля сопоставляется модуль сети. На подстранице этого N-модуля располагается сеть, которая отображает структуру тела E-модуля и содержит по одному N-модулю для каждого из модулей-наследников, описанных в E-модуле. Для каждого из наследников процедура повторяется.

В **разд. 2.3** рассматривается моделирование формальных параметров и экспортируемых переменных. Каждый параметр или переменная представляются местом на странице тела модуля-родителя. Это место соединяется с N-модулем, соответствующим E-модулю, где описан параметр или переменная.

Разд. 2.4 посвящен отображению структуры связей. Каждая точка взаимодействия E-модуля представляется двумя местами, одно из которых представляет очередь исходящих сообщений, а второе — очередь сообщений, полученных E-модулем через точку взаимодействия. Места, которые представляют две точки взаимодействия, связанные каналом, сливаются между собой таким образом, чтобы сохранялось направление передачи сообщений.

В **разд. 2.5** описывается моделирование тела E-модуля. Каждая переменная представлена на странице тела E-модуля одним местом. Начальная разметка мест на странице тела E-модуля определяется разделом инициализации спецификации. Каждому E-переходу, описанному в теле E-модуля, сопоставляется N-модуль. Если E-переход использует какой-нибудь ресурс (переменную, параметр или точку взаимодействия), то место, представляющее этот ресурс, соединяется с соответствующим N-модулем.

Разд. 2.6 посвящен отображению E-переходов. Блок E-перехода разбивается на подблоки, каждый из которых является вызовом процедуры или функции, условным оператором, циклом или простым блоком, т.е. последовательностью операторов присваивания и передачи сообщения, ни один из которых не использует переменной, ранее измененной в этом же блоке. Каждый подблок рассматривается отдельно, ему сопо-

ставляется фрагмент сети. Фрагменты последовательно соединяются с помощью служебных мест.

Вызов процедуры или функции представляется N-модулем. Тело процедуры/функции отображается в сеть по той же схеме, что и блок перехода. При отображении условных операторов и циклов используются библиотечные фрагменты сети. Разбиение подблоков прекращается по достижении простого блока, который моделируется одним N-переходом. Места, представляющие используемые простым блоком ресурсы, становятся входными и выходными для этого перехода, входящие в блок операторы преобразуются в выражения на дугах.

Разд. 2.7 содержит описание моделирования отложенных E-переходов. Подсеть, моделирующая E-переход с задержкой, состоит из трех частей: 1-я часть представляет приставку `provided`, 2-я реализует механизм задержки E-перехода, а 3-я — блок E-перехода. Время задержки E-перехода отсчитывается переходом *timer*, интервал срабатывания которого совпадает с интервалом, указанным в приставке `delay`.

В **разд. 2.8** рассматривается организация такта вычисления. Для каждой подсистемы создается конструкция, которая связывает все страницы, моделирующие подсистему, и реализует правило выбора E-перехода для выполнения.

В **разд. 2.9** приводится обоснование алгоритма, предложенного во второй главе, и оценка размера результирующей сети.

Утверждение 1. Сеть, получающаяся в результате отображения Estelle-спецификации, безопасная.

Состояние E-модуля и разметка моделирующей его сети называются *эквивалентными* при следующих условиях:

– значение фишки в месте *State* совпадает с текущим локальным состоянием E-модуля;

– для каждой точки взаимодействия E-модуля число сообщений в очереди этой точки совпадает с длиной списка в соответствующем месте, и порядок сообщений совпадает;

– для каждой переменной ее значение и значение фишки в месте, моделирующем эту переменную, равны.

Утверждение 2. Если E-переход возможен из некоторого состояния E-модуля, то в сети из эквивалентной разметки может произойти

последовательное срабатывание всех переходов, входящих в сеть, которая моделирует этот E-переход. Полученные таким образом состояние и разметка будут снова эквивалентны.

Пусть E-модуль содержит var переменных, ip точек взаимодействия, par параметров и t переходов. Среди общего числа n операторов E-модуля выделим c вызовов процедур и функций и k операторов, для моделирования которых заведомо требуется более одного перехода. Через $att = var + 1 + 2 * ip + par$ обозначим число "значимых" мест.

Утверждение 3. Сеть, моделирующая E-модуль, может иметь не более TN переходов и PN мест, где $TN = (n + 4k) * (c + 1) + 4t$, $PN = (n + att + 4k) * (c + 1) + 5t$.

В **третьей главе** предлагается алгоритм отображения динамических Estelle-спецификаций в РСП, расширенных приоритетами и временным механизмом Йенсена. Рассматриваются только спецификации, допускающие последовательное недетерминированное поведение. Подход основан на том, что текстуальная вложенность описаний модулей образует статический шаблон спецификации. Число экземпляров модуля может изменяться в процессе выполнения, но позиция в общей иерархии фиксирована. При моделировании Estelle-спецификации статическая структура сети представляет иерархию описаний. Экземпляры модулей моделируются фишками, число которых изменяется при создании или уничтожении экземпляров модулей.

Разд. 3.1 посвящен построению дерева страниц моделирующей сети. Правила в целом подобны описанным в разд. 2.2, но элементы сети сопоставляются не конкретному экземпляру, а описанию E-модуля определенного типа. Заголовку E-модуля сопоставляется один N-модуль, на подстранице которого создается по одному N-модулю для каждого тела E-модуля. Внутренняя структура тела E-модуля моделируется на подстранице N-модуля, представляющего это тело.

В **разд. 3.2** обсуждается проблема идентификации экземпляров модулей. Фишки, принадлежащие разным экземплярам, снабжаются уникальным признаком — персональным идентификатором модуля (ПИМ). Все фишки, принадлежащие одному экземпляру модуля, помечены одним и тем же ПИМ.

В **разд. 3.3** рассматривается моделирование формальных парамет-

ров и экспортируемых переменных E-модуля. От статического случая его отличают правила порождения множеств цветов и выражения на дугах: всюду хранится и передается не просто значение соответствующего типа, а пара (ПИМ, значение).

Разд. 3.4 посвящен отображению точек взаимодействия. Точка взаимодействия E-модуля представляется тремя местами. К двум местам, представляющим очереди входящих и исходящих сообщений, добавляется место IP_info, которое служит для хранения информации о том, какие связи установлены для точки взаимодействия `IP`.

В **разд. 3.5** и **3.6** описывается моделирование операторов установления и разрыва связей соответственно. Так как связи между точками могут изменяться, слияния мест, содержащих очереди сообщений, не происходит. Связь между точками взаимодействия, которая может возникнуть в процессе функционирования спецификации, представляется двумя переходами. Каждая пара переходов моделирует перемещение сообщений по соединяющему точки каналу. Установление и разрыв связей изменяют значения фишек в местах IP_info для точек взаимодействия, между которыми была создана или уничтожена связь.

В **разд. 3.7** рассматривается организация ввода/вывода с учетом того, что E-модуль может иметь доступ к очередям точки взаимодействия только в том случае, если эта точка является концом линии связи.

Разд. 3.8 посвящен моделированию тела E-модуля. Каждому типу модулей-наследников, описанных в теле, сопоставляется N-модуль, отображаются точки взаимодействия и возможные связи между ними. Для каждого типа модулей-наследников `T` создаются места T_inst, T_init и T_kill. Место T_inst хранит информацию о существующих на данный момент экземплярах модулей типа `T`, а места T_init и T_kill используются при создании и уничтожении экземпляров модулей этого типа. Построение той части сети, которая определяет функционирование E-модуля, в целом подобно статическому случаю.

В **разд. 3.9** описывается отображение E-переходов. Рассматриваются библиотечные фрагменты, моделирующие операторы `all`, `forone` и `exist`, которые позволяют оперировать с экземплярами модулей-наследников. Обсуждается структура сети, моделирующей отложенные E-переходы в терминах временной модели Йенсена.

В **разд. 3.10** рассматривается создание и уничтожение экземпляров E-модулей. Создание нового экземпляра некоторого типа заключается в размещении по всем "значимым" местам сети, моделирующей тело E-модуля, набора фишек, который помечен новым ПИМ. Уничтожение экземпляра представляет собой обратное действие. Из мест сети удаляются все фишки, которые помечены ПИМ, полученным от модуля-родителя.

В **разд. 3.11** обсуждается моделирование такта вычисления. Дополнительная конструкция, которая связывает все страницы, моделирующие подсистему, структурно не отличается от используемой в статическом случае. Однако при моделировании такта вычислений используется временной механизм. Начало нового такта вычислений откладывается на некоторое время, в течение которого происходит моделирование передачи сообщений, проверка условий возможности E-переходов, а также включение и выключение таймеров.

В **разд. 3.12** приводится обоснование предложенного алгоритма и оценка размера результирующей сети. Моделирующая сеть называется *послойно безопасной*, если все места, относящиеся к одному модулю, за исключением мест T_inst, содержат не более одной фишки, принадлежащей одному и тому же экземпляру.

Утверждение 4. Сеть, полученная в результате отображения Estelle-спецификаций, содержащих динамические конструкции, послойно безопасна.

Состояние E-модуля и разметка моделирующей его сети называются *эквивалентными* при следующих условиях:

– выполняются условия эквивалентности, приведенные в разд. 2.9;

– фишки в местах IP_info описывают текущую структуру связей согласно правилам, описанным в разд. 3.4–3.6;

— каждый модуль-наследник `M` типа `T` представлен в месте T_inst фишкой, содержащей информацию о типе тела и ПИМ экземпляра наследника.

Утверждение 5. Если E-переход возможен из некоторого состояния E-модуля, то в сети из эквивалентной разметки может произойти последовательное срабатывание всех переходов, входящих в сеть, которая моделирует этот E-переход. Полученные таким образом состояние

и разметка будут снова эквивалентны.

Пусть E-модуль содержит var переменных, ip точек взаимодействия, par параметров и t переходов. Среди общего числа n операторов E-модуля выделим c вызовов процедур и функций и k операторов, для моделирования которых заведомо требуется более одного перехода. Число "значимых" мест в модуле будет равно $att = var + 7 + 5 * ip + par$.

Утверждение 6. Сеть, моделирующая E-модуль, может иметь не более TN переходов и PN мест, где $TN = (n + 5k) * (c + 1) + 2t$, $PN = (n + att + 4k) * (c + 1) + 4t$.

В **четвертой главе** в **разд. 4.1** описана система EPV, представляющая собой интегрированный программный комплекс для проектирования, анализа и симуляции сетевых моделей распределенных систем. В качестве сетевых моделей используются ИВТ-сети, являющиеся вариантом раскрашенных сетей. В ИВТ-сетях используется концепция времени, предложенная Мерлином, допускается тип массив и могут присутствовать места-очереди, где новая фишка "помещается в очередь" и остается недоступной, пока из места не будут извлечены все фишки, поступившие до нее.

Основными компонентами комплекса являются транслятор, конвертор, графический редактор и симулятор. Транслятор осуществляет автоматический перевод Estelle-спецификации во внутреннее представление ИВТ-сети. Конвертор переводит ИВТ-сети в текстовое представление, являющееся входным для системы Design/CPN. Таким образом, система EPV позволяет использовать средства анализа системы Design/CPN. Средствами многооконного графического редактора ИВТ-сетей осуществляется построение и изменение сетевой модели и контроль структурной корректности иерархических сетевых моделей. Симулятор интегрирован с редактором и визуализирует функционирование ИВТ-сетей, а также позволяет протоколировать сеанс симуляции.

В **разд. 4.2** описаны эксперименты с кольцевым протоколом RE, представленным на языке Estelle. RE-протокол предназначен для сетей, в которых несколько станций соединяются однонаправленными каналами в кольцо. По кольцу циркулирует *фрейм*, который служит для передачи данных между станциями. Любая станция в произвольный момент времени может покидать кольцо или возвращаться в него. Когда стан-

ция покидает кольцо, разрыва кольца не происходит: кадр передается сквозь нее далее по кольцу.

Для управления доступом к фрейму RE-протокол использует первые два бита фрейма в качестве *метки* и предполагает, что одна из станций выполняет роль *монитора*, контролируя правильность операций с меткой. Во время экспериментов с RE-протоколом досконально изучалось восстановление функционирования кольца после ошибки передачи. При этом было обнаружено, что станция-немонитор может распознавать пострадавший в результате ошибки передачи кадр как содержащий адресованное ей данное. Такая ситуация возникает, если в пустом фрейме изменяется значение второго бита метки, "превращая" его в полный. Вероятность такой ситуации значительно снижается, если при освобождении фрейма обнулять не только поле, содержащее личный номер станции-отправителя, но и поле, содержащее номер станции-получателя.

В **приложении** приведена Estelle-спецификация RE-протокола.

Основные выводы и результаты

В рамках диссертации были получены следующие результаты.

• Разработан алгоритм перевода статических Estelle-спецификаций с задержками и приоритетами в расширенную модель раскрашенных сетей. Доказано, что алгоритм дает безопасные сети. Дано обоснование предложенного алгоритма. Получены верхние оценки размера моделирующей сети, подтверждающие эффективность алгоритма.

• Разработан способ моделирования Estelle-спецификаций с динамическими конструкциями и алгоритмы перевода последних в раскрашенные сети Петри. Для моделирующей сети доказан аналог свойства безопасности. Дано обоснование предложенного алгоритма. Приведена оценка размера моделирующей сети.

• Метод перевода статических Estelle-спецификаций адаптирован для модели ИВТ-сетей, реализованной в системе EPV. Проведены эксперименты по поиску семантических ошибок в коммуникационных протоколах. В ходе экспериментов с кольцевым протоколом, известным как RE-протокол, обнаружена неэффективность в поведении протокола. Предложено исправление протокола, устраняющее эту неэффективность.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. **Окунишникова Е. В.** Отображение Estelle-спецификаций в раскрашенные сети Петри и его обоснование. — Новосибирск, 2001. — 59 с. — (Препр./Сиб. отд-ние РАН. ИСИ; N 90)

2. **Непомнящий В. А., Алексеев Г. И., Быстров А. В., Мыльников С. П., Окунишникова Е. В., Чубарев П. А., Чурина Т. Г.** Верификация коммуникационных протоколов, представленных на языке Estelle, с помощью сетей Петри высокого уровня // Программирование. — 2001. — N. 2. — С. 5–20.

3. **Окунишникова Е. В.** Моделирование Estelle-спецификаций посредством раскрашенных сетей Петри // Тр. конф. молодых ученых, посвященной 10-летию ИВТ СО РАН. Т. I: Информационные технологии, задачи поддержки принятия решений. — Новосибирск: Ин-т вычислит. технологий СО РАН, 2001. — С. 59–61.

4. **Окунишникова Е. В.** Моделирование Estelle-спецификаций посредством раскрашенных сетей Петри // Тез.докл. IV сибирского конгресса по прикладной и индустриальной математике (ИНПРИМ-2000): — Новосибирск: Ин-т математики СО РАН, 2000. — С. 124.

5. **Непомнящий В. А., Алексеев Г. И., Быстров А. В., Мыльников С. П., Окунишникова Е. В., Чубарев П. А., Чурина Т. Г.** Верификация коммуникационных протоколов, представленных на языках Estelle и SDL // Там же. — С. 123.

6. **Окунишникова Е. В.** Моделирование динамических конструкций языка Estelle посредством раскрашенных сетей Петри. — Новосибирск, 2000. — 70 с. — (Препр./Сиб. отд-ние РАН. ИСИ; N 78)

7. **Алексеев Г. И., Быстров А. В., Куртов С. А., Мыльников С. П., Непомнящий В. А., Окунишникова Е. В., Чубарев П. А., Чурина Т. Г.** Использование сетей Петри для верификации распределенных систем, представленных на языке Estelle // Известия РАН. Сер. Теория и системы управления. — 1999. — N. 5. — С. 105–116.

8. **Окунишникова Е. В.** Представление временных конструкций Estelle в различных моделях временных сетей Петри. — Новосибирск, 1999. — 32 с. — (Препр./Сиб. отд-ние РАН. ИСИ; N 70)

9. **Непомнящий В. А., Алексеев Г. И., Быстров А. В., Куртов С. А., Мыльников С. П., Окунишникова Е. В., Чубарев П. А., Чурина Т. Г.** Верификация Estelle-спецификаций распределенных систем посредством раскрашенных сетей Петри. — Новосибирск: ИСИ СО РАН, 1998. — 140 с.

10. **Churina T. G., Okunishnikova E. V.** Modelling Estelle specifications using Coloured Petri nets.// Joint Bulletin of the NCC and the IIS . Ser. Computer Science. — 1998. — N 8. — P. 19–39.

11. **Nepomniaschy V. A., Alekseev G. I., Bystrov A. V., Churina T. G., Mylnikov S. P.,Okunishnikova E. V.** Towards Verification of Estelle-specified Communication Protocols: Coloured Petri Net Approach // Proc. Int. Conf. on Parallel Computing in Electrical Engineering. — Bialystok, Poland, 1998, P. 141–147.

12. **Nepomniaschy V. A., Alekseev G. I., Bystrov A. V., Churina T. G., Mylnikov S. P., Okunishnikova E. V.** EPV — Petri Net Based Estelle Protocol Verifier // Proc. 1st Internati. Workshop on the Formal Description Technique Estelle. — Evry, France, 1998. — P. 101–108.

13. **Churina T. G., Okunishnikova E. V.** Coloured Petri nets approach to the validation of Estelle specifications // Proc. of Workshop on Concurrency, Specification and Programming. — Warsaw, Poland, 1997. — P. 25—36.

14. **Nepomniaschy V. A., Alekseev G. I., Bystrov A. V., Churina T. G., Mylnikov S. P., Okunishnikova E. V.** Petri net modelling of Estelle-specified communication protocols // Proc. 3rd Int. Conf. Parallel Computing Technologies. — Berlin a. o.: Springer-Verlag, 1995. — P. 94—108. — (Lect. Notes Comput. Sci., Vol. 964).

15. **Окунишникова Е. В., Чурина Т. Г.** Способ построения раскрашенных сетей Петри, моделирующих Estelle-спецификации // Проблемы спецификации и верификации параллельных систем. — ИСИ СО РАН, Новосибирск, 1995. — С. 95—123.

16. **Nepomniaschy V. A., Churina T. G., Okunishnikova E. V.** Translation of Estelle protocol specification in coloured Petri nets. Extended Abstract // Proc. IFIP 15th Intern. Sympos. on Protocol Specification, Testing and Verification. — Warsaw, Poland, 1995. — P. 447—450.

Личный вклад автора

Все включенные в диссертацию результаты, касающиеся моделирования динамических возможностей Estelle, получены автором самостоятельно. В работах по моделированию статических Estelle-спецификаций, выполненных в соавторстве, Е. В. Окунишникова внесла следующий вклад: разработано отображение в РСП точек взаимодействия модулей Estelle и связей между ними, моделирование E-переходов с простым блоком, а также процедур и функций; разработаны принципы представления в сети временных конструкций Estelle; доказана безопасность моде-

лирующей сети, обоснована корректность алгоритма построения, даны оценки размера моделирующей сети; на основании разработанного алгоритма выделен эффективный подкласс РСП, получивший название ИВТ-сетей, использованный в дальнейшем при создании системы EPV; проведены и описаны эксперименты с кольцевым протоколом.

Окунишникова Елена Валерьевна

МОДЕЛИРОВАНИЕ ESTELLE-СПЕЦИФИКАЦИЙ РАСПРЕДЕЛЕННЫХ СИСТЕМ С ПОМОЩЬЮ РАСКРАШЕННЫХ СЕТЕЙ ПЕТРИ

Подписано в печать 27.07.04 Объем 1,0 уч.-изд.л.
Формат бумаги 60×84 1/16 Тираж 100 экз.

ЗАО РИЦ "Прайс-курьер" 630090, г. Новосибирск, пр. Акад. Лаврентьева, 6, тел. (383-2) 34-22-02