УДК 681.3
Ю.К. Апраксин, профессор, д-р техн. наук,
А.И. Копылова
Севастопольский национальный технический университет
ул. Университетская 33, г.Севастополь, Украина, 99053
E-mail: kvt@sevntu.sebastopol.ua

ВАЛИДАЦИЯ ПРОТОКОЛОВ РАСПРЕДЕЛЁННЫХ СИСТЕМ, ПРЕДСТАВЛЕННЫХ КОНЕЧНО - АВТОМАТНОЙ МОДЕЛЬЮ

Предлагается подход к валидации протоколов распределённых систем, представленных конечно-автоматной моделью. В качестве метода контроля корректного функционирования системы выбран анализ дерева достижимых глобальных состояний.

***Ключевые слова**: валидация, распределённая система, дерево достижимых глобальных состояний, конечный автомат.*

В целях обеспечения совместного использования ресурсов многокомпьютерной системы необходимо организовать взаимодействие независимых и в то же время информационно связанных между собой компьютеров в единое целое. Подобные системы обычно называются распределёнными (РС) [1]. Обмен данными в таких системах сводится к передаче сообщений от одного объекта системы к другому. Управляют обменом специальные протоколы: аппаратные, программные или аппаратно-программные средства, реализующие алгоритм и формат обмена [2]. Наиболее подходящей абстрактной моделью протокола является расширенный конечный автомат [3], который в дальнейшем будем называть протокольным автоматом (ПА).

Целью настоящей работы является формирование модели протоколов РС, обеспечивающих возможность автоматической процедуры валидации, под которой понимается проверка функционирования системы на соответствие требованиям заказчика.

ПА определяет взаимодействие, как минимум, двух процессов. Описание такой модели можно представить в виде пары взаимодействующих протокольных автоматов $ПА_i$ и $ПА_j$:

$ПА_i :: <\{\{+m_{ji}\} \cup \{-m_{ij}\}\}, \{P_i^k\}, P_i^0, \gamma_i = \gamma_i(P_i^k, \pm m^k_{ij}), F_i >$;

$ПА_j :: <\{\{+m_{ij}\} \cup \{-m_{ji}\}\}, \{P_j^r\}, P_j^0, \gamma_j = \gamma_j(P_j^r, \pm m^r_{ji}), F_j >$.

Здесь введены следующие обозначения:

$\{+m_{ji}\}(\{+m_{ij}\})$ – сообщения, принимаемые $ПА_i$ ($ПА_j$) от $ПА_j$($ПА_i$);

$\{-m_{ij}\}(\{-m_{ji}\})$ – сообщения, посылаемые $ПА_i$ ($ПА_j$) к $ПА_j$($ПА_i$);

$\{P_i^k\}$ – множество процессов ($k = 1,2,\ldots,K$), реализующих сервис протокола $ПА_i$;

$\{P_j^r\}$ – множество процессов ($r = 1,2,\ldots,R$), реализующих сервис протокола $ПА_j$;

P_i^0 (P_j^0) – начальные (активизирующие) процессы $ПА_i$ ($ПА_j$);

γ_i (γ_j) – функции выходов, определяющие каким процессом $ПА_i$ ($ПА_j$) формируется сообщение-посылка к $ПА_j$($ПА_i$);

F_i (F_j) – совокупность процессов $ПА_i$ ($ПА_j$), завершающих формирование сервиса.

Каждое состояние ПА интерпретируется как внутренний процесс обработки или формирования сообщений. Передача сообщений осуществляется через коммуникационную среду. Модель этой среды в общем случае представляет собой совокупность очередей с известной системой обслуживания. Например, если два процесса обмениваются сообщениями через полудуплексный канал и дисциплина обслуживания очереди сообщений C_{ij} (передача от $ПА_i$ к $ПА_j$) и C_{ji} (передача от $ПА_j$ к $ПА_i$) определяется как FIFO (First Input – First Output), то описание модели канала можно представить тремя правилами функционирования:

– посылка сообщения

$$P_i' = \gamma_i(P_i, -m);\ C'_{ij} = C_{ij}.m;\ \ P_j' = \gamma_j(P_j, -m);\ C'_{ji} = C_{ji}.m;$$

– приём сообщения

$$P_i' = \gamma_i(P_i, +m);\ C_{ij} = m.C'_{ij};\ \ P_j' = \gamma_j(P_j, +m);\ C_{ji} = m.C'_{ji};$$

– внутреннее событие без посылки, либо приёма сообщений (таймаут)

$$P_i' = \gamma_i(P_i, \oslash);\ C'_{ij} = C_{ij};\ \ P_j' = \gamma_j(P_j, \oslash);\ C'_{ji} = C_{ji}.$$

Здесь C'_{ij}, P_i', C'_{ji}, P_j' – состояния каналов и ПА после завершения события.

Предложенная модель позволяет определять текущее состояние системы взаимодействия двух объектов РС как (P_i, C_{ij}, P_j, C_{ji}), которое будем называть глобальным состоянием.

Модель глобального состояния РС, состоящей из N взаимодействующих объектов, можно представить квадратной матрицей $(PC)_{N\times N}$, диагональные элементы которой определяют локальные

состояния $ПА_i$ ($i = 1,2,\ldots,N$), а на пересечении i-ой строки и j-го столбца фиксируется состояние канала связи C_{ij}.

Для реализации задачи валидации протоколов используется метод анализа дерева достижимых глобальных состояний (ДДГС) [3]. Корневой вершиной ДДГС является начальное глобальное состояние (P_i^0, $C_{ij} = \varnothing$, P_j^0, $C_{ji} = \varnothing$). Переход на новую (текущую) вершину определяется событием, реализуемым текущим процессом P_i^k (P_j^r). Валидация выполняется путем обхода ДДГС от корневой вершины до листьев дерева. Если обнаруживается несоответствие, то вершины данной ветви, расположенные ниже, уже не анализируется. Из этого можно сделать вывод, что время выполнения задачи валидации системы тем быстрее, чем ближе к корневой вершине ДДГС обнаруживается несоответствия спецификации. Максимальное время решения задачи валидации наблюдается при полном соответствии функционирования системы требованиям заказчика.

Рассмотрим пример валидации системы «клиент – банкомат». Валидация определяет наличие таких свойств протокола:

- полнота – все переходы исходной спецификации «системы протокольного взаимодействия» отражены в ДДГС;
- завершаемость – все терминальные вершины ДДГС имеют формат конечного состояния ($F_i, \varnothing$, $F_j, \varnothing$);
- отсутствие неспецифицированных приёмов сообщений: для любого глобального состояния (P_i^k, $m_{ij}C'_{ij}$, P_j^r, $m_{ji}C'_{ji}$) в исходной спецификации должны существовать переходы типа $P_i' = \gamma_i(P_i, \pm m_{ij})$ или $P_j' = \gamma_j(P_j, \pm m_{ji})$;
- отсутствие бесполезных циклов, циклов, из которых нет ни одного перехода в новое состояние, за исключением устойчивых состояний;
- безызбыточность – для любого состояния ДДГС должны существовать переходы, определённые в графической интерпретации взаимодействующих протокольных автоматов;
- соблюдение требований, ограничивающих ёмкость канала.

На рисунке 1 изображена графическая интерпретация взаимодействующих $ПА_1$ и $ПА_2$. Рисунок 2 иллюстрирует построение ДДГС.

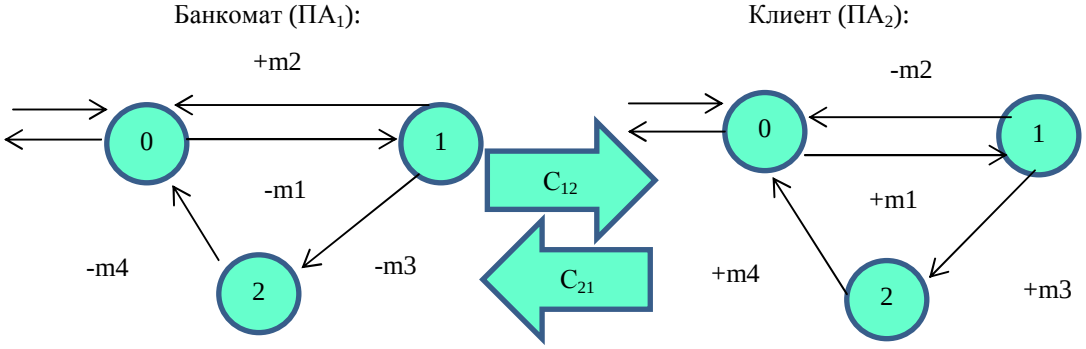

Рисунок 1 – Исходное представление системы протокольного взаимодействия «$ПА_1$ – $ПА_2$»

Начальное и конечное состояние – оба автомата находятся в состоянии 0 и очереди пустые, т.е. при достижении этого состояния клиент может выйти из системы.

Построение дерева достижимых глобальных состояний показано на рисунке 2.

Описание протокольных автоматов приведено в таблицах 1, 2.

Таблица 1 – Описание состояний протокольных автоматов

Состояние	Банкомат	Клиент
1	Начальное состояние	Начальное состояние Клиенту необходимо ввести карточку, PIN – код или выйти из системы
2	Активное состояние автомата (можно выбирать выполнение какой либо операции)	Клиенту необходимо выбрать необходимую операцию
3	Выполнение операции	Выполнения операции

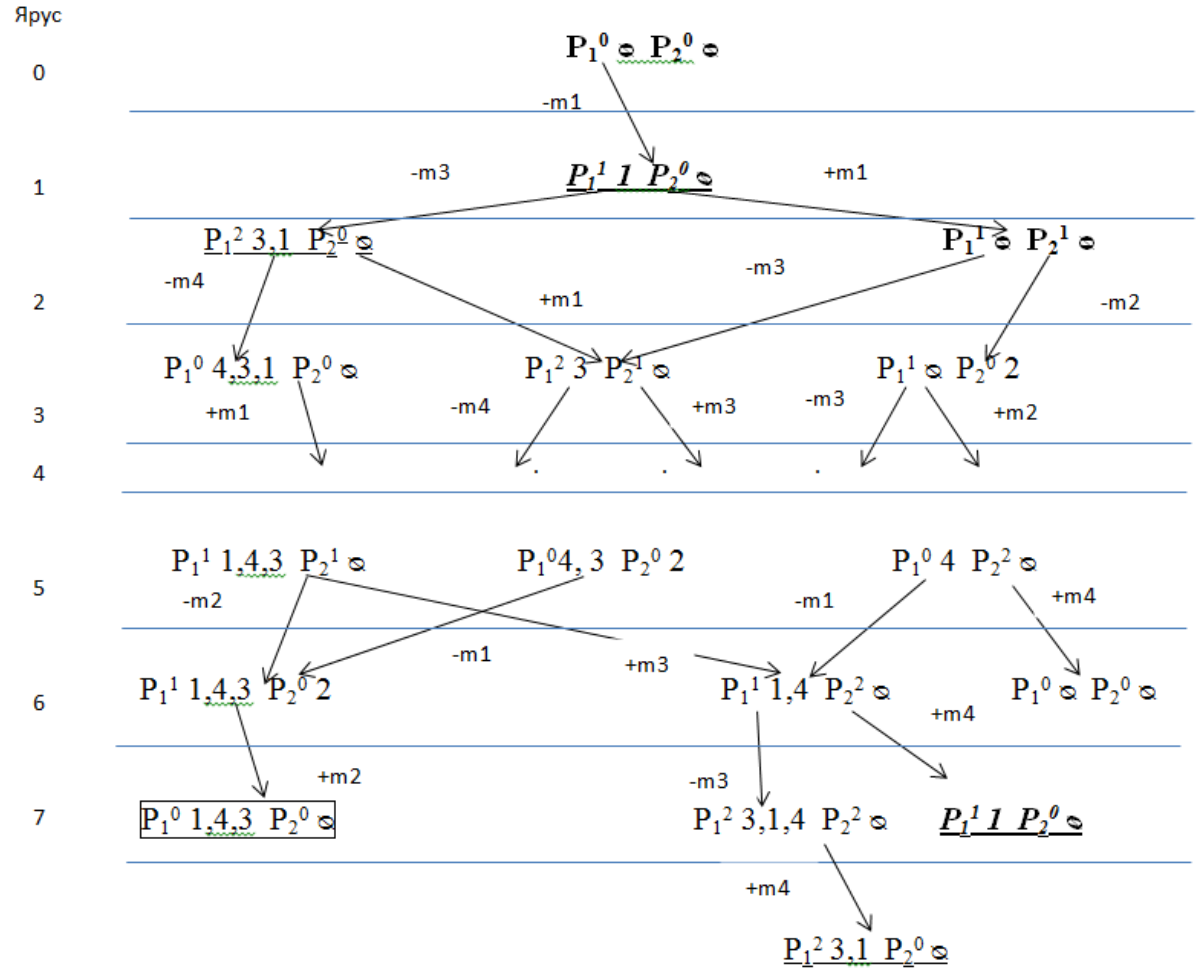

Рисунок 2 – Фрагмент ДДГС

Таблица 2 – Описание передаваемых \ принимаемых сообщений

Сообщения «Банкомата»	Описание сообщения	Сообщение «Клиента»	Описание сообщения
-m1	Вставьте карточку и введите PIN-код	+m1	Клиент принимает сообщение «-m1» и выполняет требуемые действия (не принимая это сообщение клиент может выйти из системы)
+m2	При принятии сообщения «-m2», банкомат переходит в начальное состояние	-m2	Прервать операцию
-m3	Выберете необходимую операцию	+m3	Клиент выбирает необходимую операцию
-m4	Уведомление об окончании выполнения операции	+m4	При принятии этого сообщения автомат приходит в начальное состояние. Если работу необходимо продолжить, то осуществляется приём следующего сообщения, если нет – банкомат прекращает свою работу

При анализе ДДГС можно выделить следующее состояние: в ДДГС есть вершина (на 7 ярусе), из которой не выполняется передача \ приём сообщений из-за соблюдения требований, ограничивающих ёмкость канала. При увеличении объёма очереди увеличится и глубина дерева, однако подобные состояния также останутся. На ярусах 3,5,6 и 7 есть состояния, из которых осуществляется переход в другие состояния, которые находятся на верхних ярусах, что свидетельствует о возможности

возникновения циклов, но в данном случае циклы не бесполезные – система всё равно переходит в конечное состояние.

В заключение рассмотрим созданную программную систему валидации сетевых протоколов, представленных в виде конечной автоматной модели. Программа написана на языке Java с использованием технологий соответствующих платформ. Для работы программы необходимо сначала задать в файлах описание взаимодействующих объектов с помощью таблицы переходов и выходов, а также ограничение на длину очереди. В результате валидации программа выводит информацию о созданной модели в текстовое поле интерфейса программы, в котором отражаются сообщения об несоответствиях модели требованиям заказчика или об успешной валидации модели.

В дальнейшем на основе разработанного приложения планируется выполнить валидацию модели, которая будет реализована в результате взаимодействия большего количества объектов, реализовать обслуживание очереди другими методами(LIFO, по приоритетам и др.), использовать дуплексный режим взаимодействия протокольных автоматов и сравнить полученные результаты по производительности; выполнить валидацию конкретного протокола.

Библиографический список использованной литературы

1. Таненбаум Э. Распределённые системы. Принципы и парадигмы / Э. Таненбаум, М. ван Стеен. — СПб.: Питер, 2003. — 877 с.

2. Протоколы информационно-вычислительных сетей: справочник / под ред. И.А. Мизина, А.П. Кулешова. — М.: Радио и связь, 1990. — 504 с.

3. Апраксин Ю.К. Моделирование поведения взаимодействующих объектов распределённых систем / Ю.К.Апраксин // АСУ и приборы автоматики. — Харьков, 1999. — Вып. 110. — С. 3–6.

Поступила в редакцию 12.05.2011 г.

Апраксін Ю.К., Копилова А.І. Валідація протоколів розподілених систем, представлених кінцево-автоматною моделлю

Пропонується валідація протоколів розподілених систем, представлених кінцево-автоматною моделлю. Як метод контролю коректного функціонування системи обрано аналіз дерева досяжних глобальних станів.

Ключові слова: валідація, розподілена система, дерево досяжних глобальних станів, кінцевий автомат.

Apraksin Yu.K., Kopylova A.I. The finite state automate model for distributed system protocol validation

A method for validation of protocols for distributed systems presented by finite-automate model is suggested. The analysis of the tree of reachable global states is selected as a method of monitoring the correct functioning.

Keywords: validation, distributed system, tree of reachable global states, a finite automaton.