УДК 519.74, 681.51

Д.А. ЗАЙЦЕВ, канд. техн. наук, Е.Я. ЧОРНОГАЛА

СИНТЕЗ МОДЕЛИ ПЕТРИ И ВЕРИФИКАЦИЯ ПРОТОКОЛА ЭЛЕКТРОННОЙ КОММЕРЦИИ IOTP

Протокол электронной коммерции IOTP является наиболее сложным из более чем четырёх сотен протоколов, разработанных IETF. Его стандартная спецификация [1] занимает около трёхсот страниц и дополняется вспомогательными документами. Важность протокола для современного мира обуславливается неуклонным ростом объемов продаж, осуществляемых с его помощью [2]. Таким образом, верификация протокола IOTP представляет собой актуальную научную задачу.

Моделирование протокола IOTP раскрашенными сетями Петри [3] не позволяет применить формальные методы за исключением простой генерации пространства состояний для его верификации. Использование классических сетей Петри было затруднено ввиду большой размерности модели и практической неосуществимости инвариантного анализа [4]. Применение композиционных методов вычисления инвариантов [5,6] обеспечивает верификацию протокола IOTP за приемлемое время.

Целью настоящей работы является синтез модели Петри основной транзакции протокола IOTP Приобретение с использованием промежуточного языка взаимодействующих последовательных процессов (ВПП) [7], на основе методологии, ранее представленной в [8], а также верификация протокола композиционными методами [5,6].

1. Обзор протокола IOTP. Протокол предусматривает [1] обмен IOTP-сообщениями между субъектами, играющими определённую торговую роль (Trade Role). Предусмотрено пять основных торговых ролей: Клиент (Customer), Коммерсант (Merchant), Оператор платежей (Payment Handler), Оператор доставки (Delivery Handler), Обслуживание клиента (Merchant Customer Care Provider). Заметим, что несколько ролей могут выполняться одним субъектом одновременно.

Торговые обмены (Trading Exchanges) представляют собой конструктивы для формирования транзакций. Предусмотрено четыре торговых обмена: Предложение (Offer), Оплата (Payment), Доставка (Delivery), Аутентификация (Authentication). Для каждой торговой роли спецификация содержит схему взаимодействия ролей и подробные описания используемых элементов.

Транзакция представляет собой завершённое целенаправленное действие. Предусмотрены следующие транзакции: Приобретение (Purchase), Возмещение (Refund), Обмен Значений (Value Exchange), Аутентификация (Authentication), Возврат (Withdrawal), Депозит (Deposit), Справка (Inquiry). Основной транзакцией электронной коммерции является Приобретение.

Существенной для понимания протокола является структура IOTP-сообщения, которое представляет собой многоуровневый XML документ (рис. 1).

```
IOTP MESSAGE  <---------- IOTP Сообщение - XML Документ который
 |                        передаётся между торговыми ролями.
 |-Trans Ref Block <----- Блок описания транзакции - содержит информацию, которая
 |  |                     описывает IOTP Транзакцию and IOTP Сообщение.
 |  |-Trans Id Comp. <--- Компонент идентификации транзакции - уникально
 |  |                     идентифицирует IOTP Транзакцию. Компонент идентификации
 |  |                     транзакции является тем же самым для всех IOTP
 |  |                     Сообщений, которые составляют отдельную IOTP
 |  |                     транзакцию.
 |  |-Msg Id Comp. <----- Компонент идентификации сообщения - идентифицирует и
 |                        описывает IOTP Сообщение в пределах IOTP
 |                        Транзакции.
 |-Signature Block <----- Блок Подписи (необязательный) - содержит один либо
 |  |                     несколько Компонентов подписи и их
 |  |                     присоединённые Сертификаты.
 |  |-Signature Comp. <-- Компонент Подписи - содержит цифровые
 |  |                     подписи. Подписи могут удостоверять совокупности
 |  |                     Блока описания транзакции и ряда Торговых компонентов
 |  |                     в ряде IOTP Сообщений одной и той же IOTP
 |  |                     транзакции.
 |  |-Certificate Comp. < Компонент Сертификата (необязательный) Используется для
 |                        проверки подписи.
 |-Trading Block <------- Торговый блок - XML Элемент внутри IOTP
 |  |-Trading Comp.       Сообщения, который содержит предопределённое множество
 |  |-Trading Comp.       Торговых компонентов.
 |  |-Trading Comp.
 |  |-Trading Comp. <--- Торговые компоненты - XML Элементы внутри
 |                        Торгового блока, которые состоят из предопределённого
 |-Trading Block          множество XML элементов и атрибутов, содержащих
 |  |-Trading Comp.       информацию, требуемую для обеспечения Торгового
 |  |-Trading Comp.       Обмена.
 |  |-Trading Comp.
```

Рис 1. Стандартная структура IOTP-сообщения

Сообщение представляет собой последовательность торговых блоков (Trading Block), предварённую обязательными блоками Описания транзакции (Trans Ref Block) и Блоком подписи (Signature Block). Набор торговых блоков определяется типом торгового обмена; всего предусмотрено 18 типов торговых блоков. Блоки в свою очередь состоят из Торговых компонентов (Trading Component); спецификация определяет 21 торговых компонентов. Каждый торговый компонент собирается из определённых XML элементов с указанием их атрибутов.

Перечислим торговые компоненты, используемые в транзакции Приобретение:

- Статус (Status): содержит информацию об успешном завершении либо ошибках торговых процессов;
- Организация (Organization): содержит информацию об организациях и лицах;
- Заказ (Order): описывает заказ, содержит код заказа (ссылку на базу данных);
- Список способов платежа (Brand List): принимаемые способы платежа, сумма, протоколы платежа, ссылки на Операторав Платежа;
- Выбор способа платежа (Brand Selection): содержит описание выбранного способа платежа, протокола платежа и Оператора платежа;
- Платёж (Payment): содержит информацию о том, как осуществить платёж, временные штампы и ссылку на список допустимых способов платежа;
- Схема платежа (Payment Scheme): содержит информацию для выбранного протокола платежа (например, SET) с указанием конкретных данных;
- Квитанция платежа (Payment Receipt): содержит запись о фактически оплаченной (и полученной) сумме;
- Пояснения платежа (Payment Note): дополнительная информация, описывающая выполненный платёж;
- Доставка (Delivery): содержит информацию, описывающую, куда и как следует доставить товары и сервисы (почтой, курьером, через Интернет);
- Пояснения доставки (Delivery Note): информация, необходимая для получения товаров и сервисов при фактической доставке.

2. Принципы построения модели. Модель протокола может быть построена с различным уровнем детализации. Абстрактная модель представляет фишкой целое IOTP-сообщение. Наиболее детализированная модель обеспечивает различимое представление XML элементов и их атрибутов. В настоящей работе принят следующий компромисс между размером модели и её адекватностью объекту: различимо представлены Торговые компоненты протокола, задействованные в транзакции Приобретение. Кроме того, не рассматриваются необязательные компоненты и компоненты, связанные с безопасностью протокола.

В соответствии с методологией синтеза модели Петри [8] построим ВПП Торговых обменов, входящих в транзакцию Приобретение по схемам обменов стандартной спецификации протокола [1]. Затем построим ВПП транзакции Приобретение. Завершает построение модели синтез сети Петри по ВПП Транзакции Приобретение.

3. ВПП торговых обменов и транзакции. Следующие ВПП построены непосредственно по стандартным схемам Торговых Обменов, представленных на страницах 18-26 в [1]. Заметим, что вложенные скобки в ВПП опущены в предположении правой ассоциативности операции следования $\rightarrow$ таким образом, что $A \rightarrow B \rightarrow C = (A \rightarrow (B \rightarrow C))$.

Предложение:

$ConsumerOffer = MakeChoice \rightarrow PutOffer\,\mathrm{Re}\,quest \rightarrow GetOffer\,\mathrm{Re}\,sponse \rightarrow CheckOffer$.

$MercantOffer = GetOffer\,\mathrm{Re}\,quest \rightarrow Check\,\mathrm{Re}\,quest \rightarrow PutOffer\,\mathrm{Re}\,sponse$.

$Offer = MerchantOffer \,||\, ConsumerOffer$.

$Offer\,\mathrm{Re}\,sponce = Status \,||\, Organization \,||\, Order \,||\, Payment \,||\, Delivery$.

Оплата:

$ConsumerPayment = TradeDecision \rightarrow PutPaidFor \rightarrow GetBrandList \rightarrow SelectBrand \rightarrow PutBrandSelection \rightarrow GetPaymentAmount \rightarrow CheckPaymentAmount \rightarrow PutPayment\,\mathrm{Re}\,quest \rightarrow PaymentExchange \rightarrow Payment\,\mathrm{Re}\,sponse \rightarrow CheckPayment\,\mathrm{Re}\,seipt$

$MerchantPayment = GetPaidFor \rightarrow BrandDecision \rightarrow PutBrandList \rightarrow GetBrandSelection \rightarrow CheckBrandSelection \rightarrow PutPaymentAmount$

$PaymentHandlerPayment = GetPayment\,\mathrm{Re}\,quest \rightarrow CheckPayment\,\mathrm{Re}\,quest \rightarrow PaymentExchange \rightarrow PaymentPesponse$

$Payment = ConsumerPayment \,||\, MerchantPayment \,||\, PaymentHandlerPayment$

$PaymentAmount = Payment \,||\, Organization$

$Payment\,\mathrm{Re}\,quest = Status \,||\, Payment \,||\, Organization \,||\, PaySchemeData$

$PaymentExchange = PaySchemeData$

$Payment\,\mathrm{Re}\,sponse = Status \,||\, Pay\,\mathrm{Re}\,ceipt \,||\, PaymentNote$

Доставка:

$ConsumerDelivery = WhatDeliverDecision \rightarrow PutWhatDeliver \rightarrow GetHowDeliver \rightarrow CheckDeliveryInfo \rightarrow PutDelivery\,\mathrm{Re}\,quest \rightarrow GetDelivery\,\mathrm{Re}\,sponse \rightarrow CheckDeliveryNote$

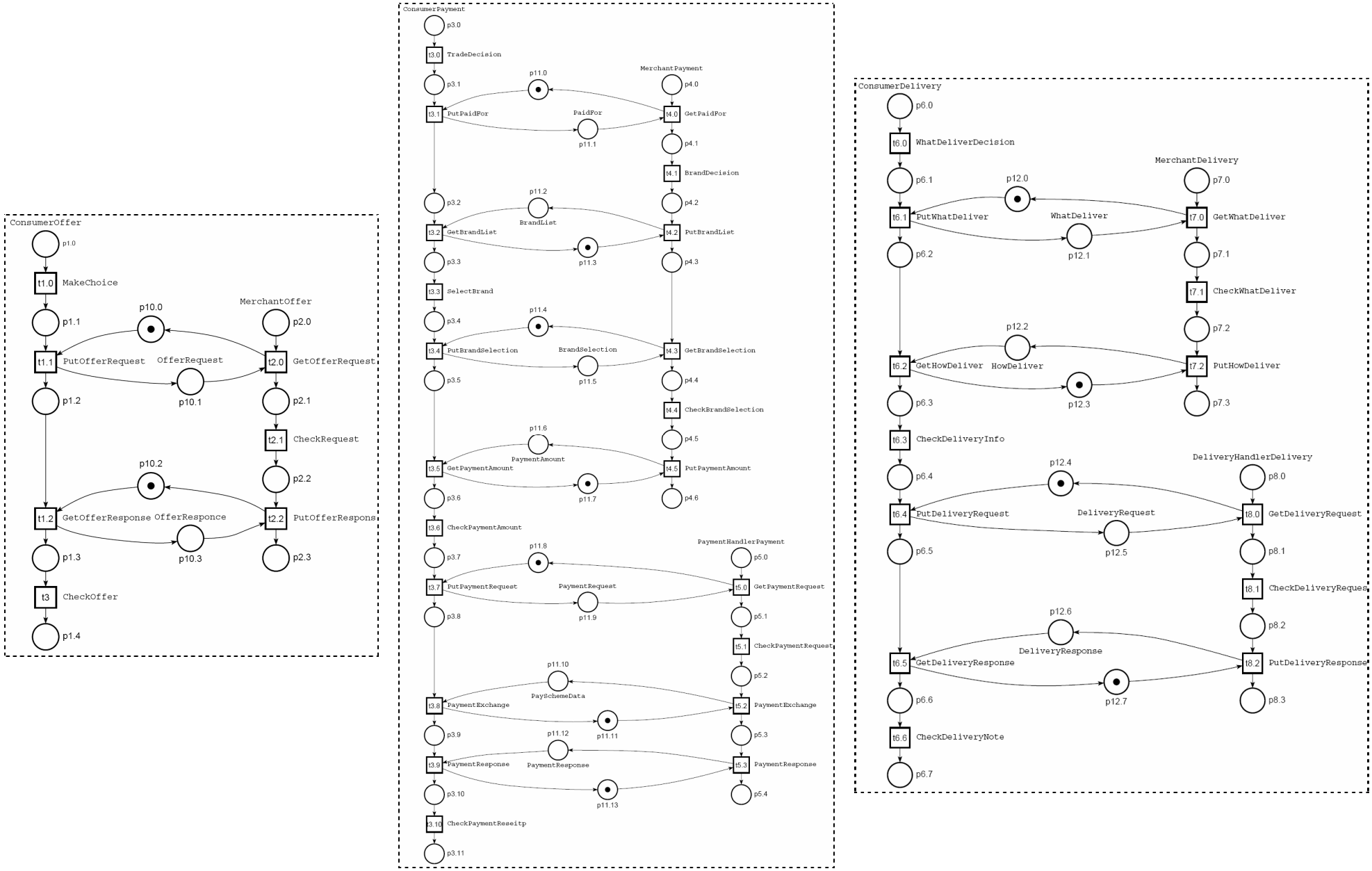

Рис. 2. Модели торговых обменов

$MerchantDelivery = GetWhatDeliver \rightarrow CheckWhatDeliver \rightarrow PutHowDeliver$

$DeliveryHandlerDelivery = GetDelivery\,\mathrm{Re}quest \rightarrow CheckDelivery\,\mathrm{Re}quest \rightarrow PutDelivery\,\mathrm{Re}sponse$

$Delivery = ConsumerDelivery \,||\, MerchantDelivery \,||\, DeliveryHandlerDelivery$

$HowDeliver = Delivery \,||\, Organization \,||\, Order$

$Delivery\,\mathrm{Re}quest = Status \,||\, Delivery \,||\, Organization \,||\, Order$

$Delivery\,\mathrm{Re}sponse = Status \,||\, DeliveryNote$

Приобретение:

$TransPerchase = Offer \rightarrow Payment \rightarrow Deliver \rightarrow TransPurchase$.

Имена переменных в формулах выбраны в соответствии с ранее описанными названиями торговых обменов, торговых ролей и компонентов. Далее приведен тезаурус имён дополнительных переменных:

- Request/Response: запрос/ответ;
- Put/Get/Check: послать/получить/проверить:
- MakeChoice: сделать выбор предложения с помощью HTTP;
- TradeDecision: принять решение о приобретаемых товарах/услугах;
- PaidFor: выбрать товары/услуги, за которые выполняется платёж с помощью HTTP;
- SelectBrand: выбрать способ платежа из списка;
- PaymentAmmount: сформировать сумму платежа;
- PaymentExchange: платёж в соответствии с выбранным способом (протоколом);
- WhatDeliverDecision: принять решение о доставляемых товарах/услугах;
- WhatDeliver: список доставляемых товаров/услуг;
- HowDeliver: описание способа доставки товаров/услуг;
- DeliveryInfo: информация о принятом к исполнению способе доставки.

4. Синтез модели Петри. Синтез модели предполагает построение отдельной сети Петри по каждой формуле ВПП и их композицию в соответствии с правилами, представленными в [8]. Модели отдельных формул являются тривиальными; их рисунки опущены. Модели торговых обменов без компонентов IOTP-сообщения изображены на рис. 2. Модель транзакции Приобретение с используемыми компонентами IOTP-сообщения представлена на рис. 3; она содержит 111 позиций и 45 переходов сети Петри. Обозначения элементов сети выбраны уникальные; пометки элементов соответствуют наименованиям переменных формул ВПП.

5. Верификация протокола. Для верификации протокола применено программное обеспечение Deborah и Adriana, реализующее вычисление инвариантов позиций и переходов сети Петри в процессе последовательной композиции её функциональных подсетей [5,6]. Инвариантный анализ классическими методами не был завершен за трое суток вычислений на компьютере Pentium 3,2GHz; композиционное вычисление инвариантов заняло около двух часов.

Граф функциональных подсетей [5,6] модели транзакции Приобретение (рис. 3) изображён на рис. 4. Вершины графа соответствуют минимальным функциональным подсетям, порождённым подмножествами переходов сети Петри; табл. 1 содержит индикаторы переходов сети Петри, указывающие номера подсетей, которым они принадлежат.

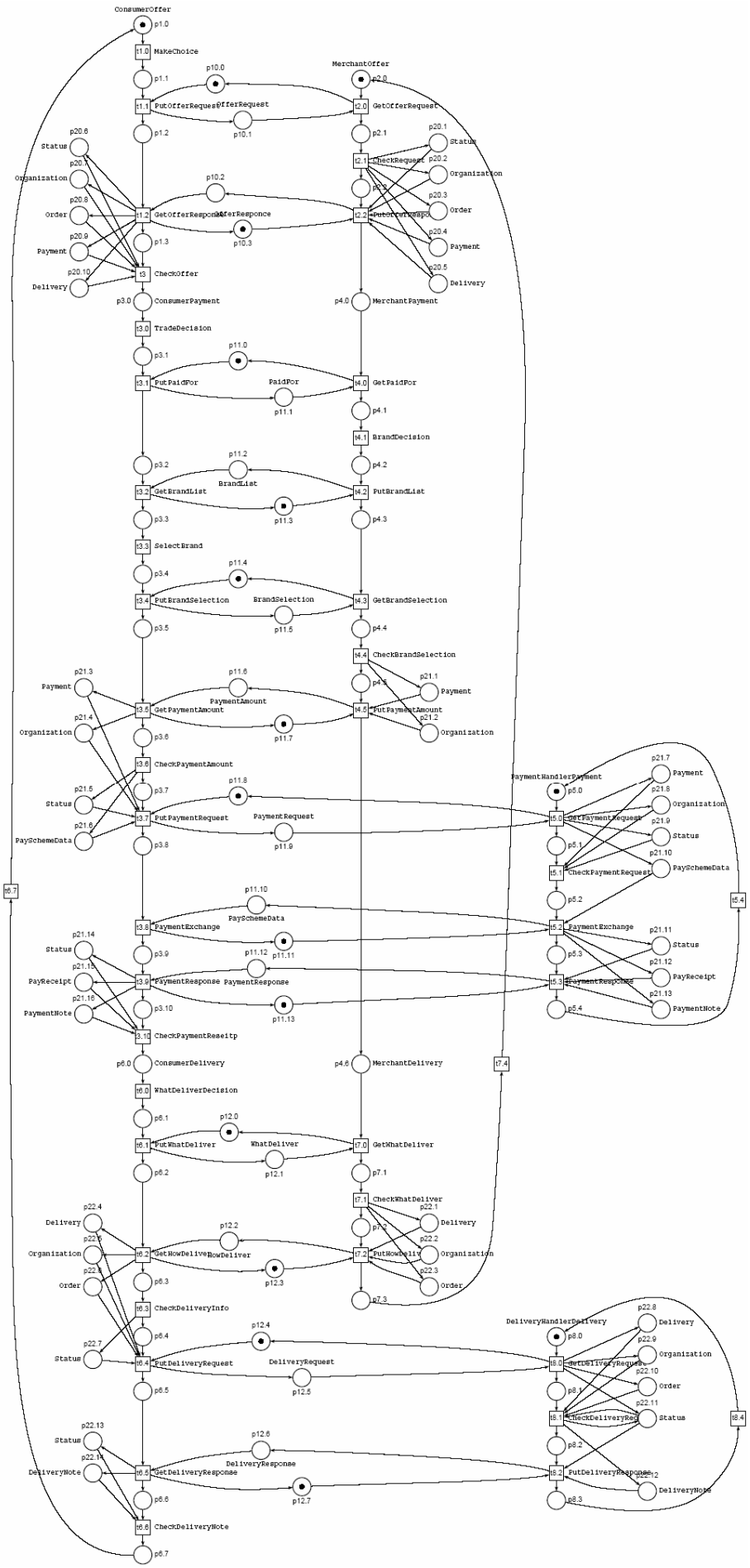

Рис. 3. Модель транзакции Приобретение

Таблица 1

Индикаторы (номеров) подсетей переходов

T	1.0	1.1	1.2	2.0	2.1	2.2	3	3.2	3.3	3.4	3.5	3.6	3.7	3.8	3.9
Z	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
T	3.10	4.0	4.1	4.2	4.3	4.4	4.5	5.0	5.1	5.2	5.3	3.0	3.1	6.0	6.1
Z	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
T	6.2	6.3	6.4	6.5	6.6	7.0	7.1	7.2	8.0	8.1	8.2	5.4	8.4	7.4	6.7
Z	31	32	33	34	35	36	37	38	39	39	39	40	41	42	43

Инвариант позиций, вычисленный программой Adriana в процессе последовательной композиции функциональных подсетей и содержащий всё ненулевые компоненты, представлен в табл. 2 (взвешенная сумма фишек равна 35). Таким образом, модель ограничена и консервативна.

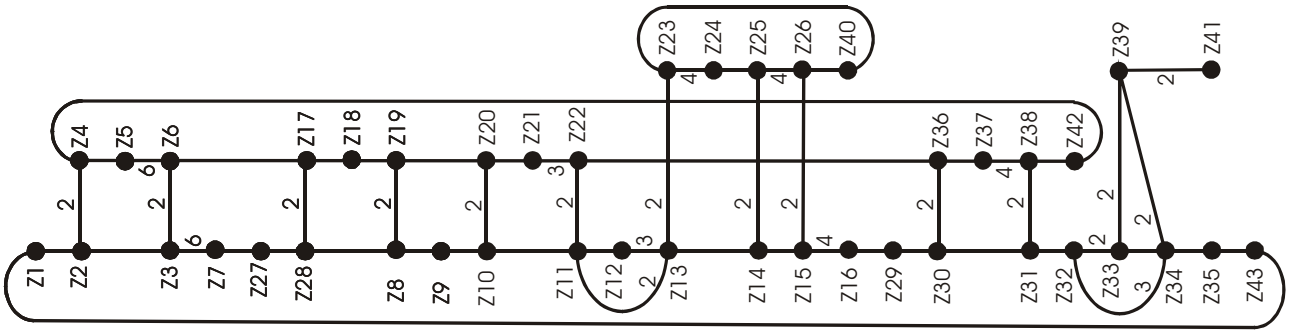

Рис. 4. Граф функциональных подсетей

Инвариант переходов, вычисленный программой Adriana в процессе последовательной композиции функциональных подсетей двойственной [4] сети Петри, содержит всё ненулевые компоненты, равные единице. Таким образом, модель имеет стационарно повторяющиеся последовательности срабатываний, содержащие все переходы, что является необходимым условием её живости.

Таблица 2

Инвариант позиций

P	p1.0	p1.1	p1.2	p2.0	p2.1	p2.2	p1.3	p3.0	p3.1	p3.2	p3.3
X(P)	6	6	6	6	6	1	1	6	6	6	6
P	p3.4	p3.5	p3.6	p3.7	p3.8	p3.9	p3.10	p4.0	p4.1	p4.2	p4.3
X(P)	6	6	4	2	6	6	3	6	6	6	6
P	p4.4	p4.5	p4.6	p5.0	p5.1	p5.2	p5.3	p5.4	p6.0	p6.1	p6.2
X(P)	6	4	6	5	1	4	2	5	6	6	6
P	p6.3	p6.4	p6.5	p6.6	p6.7	p7.1	p7.2	p7.3	p8.0	p8.1	p8.2
X(P)	3	2	6	4	6	6	1	1	5	1	3
P	p8.3	p10.0	p10.1	p10.2	p10.3	p11.0	p11.1	p11.2	p11.3	p11.4	p11.5
X(P)	5	1	1	1	1	1	1	1	1	1	1
P	p11.6	p11.7	p11.8	p11.9	p11.10	p11.11	p11.12	p11.13	p12.0	p12.1	p12.2
X(P)	1	1	1	1	1	1	1	1	1	1	1
P	p12.3	p12.4	p12.5	p12.6	p12.7	p20.1	p20.2	p20.3	p20.4	p20.5	p20.6
X(P)	1	1	1	1	1	1	1	1	1	1	1
P	p20.7	p20.8	p20.9	p20.10	p21.1	p21.2	p21.3	p21.4	p21.5	p21.6	p21.7
X(P)	1	1	1	1	1	1	1	1	1	1	1
P	p21.8	p21.9	p21.10	p21.11	p21.12	p21.13	p21.14	p21.15	p21.16	p22.1	p22.2
X(P)	1	1	1	1	1	1	1	1	1	1	1
P	p22.3	p22.4	p22.5	p22.6	p22.7	p22.8	p22.9	p22.10	p22.11	p22.12	p22.13
X(P)	1	1	1	1	1	1	1	1	1	1	1

Дополнительно верификация протокола выполнена с помощью графа достижимых маркировок [4], что подтверждает ограниченность и живость модели.

Таким образом, в настоящей работе выполнен синтез модели Петри и её верификация для транзакции Приобретение протокола электронной коммерции IOTP. Применение композиции функциональных подсетей позволило осуществить верификацию за приемлемое время. Аналогично может быть реализована верификация других транзакций протокола, а также построение и верификация моделей с уровнем детализации до XML элементов и их атрибутов, учитывающих средства обеспечения безопасности протокола.

Список литературы: 1. *FRC 2801:* Internet Open Trading Protocol - IOTP. Version 1.0E. D. Burdett, April 2000, 290p. 2. *Bidgoli H.* Electronic Commerce, Academic Press, 2002, 487p. 3. *Ouyang C., Kristensen L.M., Billington J.* A Formal and Executable Specification of the Internet Open Trading Protocol, Lecture Notes in Computer Science, Vol. 2455, Proc 3rd International Conference, EC-Web 2002, p. 377-387. 4. *Мурата Т.* Сети Петри: Свойства, анализ, приложения // ТИИЭР, т. 77, №4, 1989, с. 41-85. 5. *Zaitsev D.A.* Functional Petri Nets, Universite Paris-Dauphine, Cahier du Lamsade 224, Avril 2005, 62p. (www.lamsade.dauphine.fr/cahiers.html). 6. *Зайцев Д.А.* Последовательная композиция функциональных подсетей // Труды Одесской национальной академии связи им. А.С.Попова, № 3, 2004, с. 33-40. 7. *Хоар Ч.* Взаимодействующие последовательные процессы. М.: Мир, 1989, 264с. 8. *Зайцев Д.А.* Синтез моделей Петри телекоммуникационных протоколов // Труды Одесской национальной академии связи им. А.С.Попова, № 2, 2005, 8с.

Одесская национальная академия связи