Моделирование протоколов электронной коммерции с помощью сетей Петри (на примере протокола SET)

The e-Commerce protocol modeling using Petri nets (e.g. SET protocol)

Борхаленко Вадим Анатольевич
аспирант кафедры экономики промышленности и организации предприятия
Национальный исследовательский университет Московский энергетический институт
vadikhide@yandex.ru

Аннотация: Сеть Петри (СП) – это графическое и математическое средство моделирования систем и процессов. Формально СП представляет собой граф специального вида с дополнительными правилами, которые определяют динамику процесса функционирования СП. В данной статье представлено короткое описание моделирования процессов электронной коммерции при помощи аппарата СП. Моделируемым процессом является процесс проведения электронного платежа на базе протокола SET.

Summary: Petri net (PN) is a graphical and mathematical tool for system and process simulation. Formally PN is a graph of a special form with the additional rules that determine the dynamics of the process of functioning of the net. This report gives a brief description of developing mathematical models of e-commerce processes using PN as a tool for model development. The modeling process is the process of electronic payment transaction based on e-commerce protocol SET.

Ключевые слова: Протоколы электронной коммерции, безопасность электронных платежей,сети Петри, математическое моделирование.

Key words: e-Commerce protocols, Petri nets, electronic payment security, mathematical modeling.

Введение

В Интернете есть уже почти все, что может понадобиться для человека. Товары, услуги, общение, игры и т.д. Конечно, за некоторые услуги надо платить и чем быстрее и проще система платежей, тем лучше. Поэтому были придуманы электронные деньги. Но с развитием технологий, обеспечивающих безналичный расчет, начали развиваться методы, угрожающие корректному проведению электронных транзакций, а именно подмена информации, попытки несанкционированного доступа к активам продавца или покупателя. Одним из решений данной проблемы является SET-протокол защиты транзакций по банковским картам, проводимых через открытые сети типа Интернет.

SET предназначен только для осуществления платежа и не применяется для поиска или выбора товара. По протоколу SET транзакция производится держателем карты без непосредственного считывания данных с карты, вместо этого он предоставляет сертификат, подписанный организацией, в ведении которой находится оформление, регистрация и выдача сертификатов центром сертификации или удостоверяющим центром. Сертификат хранится на жестком диске компьютера и позволяет производить аутентификацию пользователя с помощью криптоалгоритмов с открытым ключом. В данной работе осуществление транзакции по протоколу SET описывается в виде математической модели асинхронного процесса, основанной на использовании аппарата моделирования дискретных систем – сетей Петри.

Описание проведения электронного платежа по протоколу SET

Получение сертификатов

Владелец карты направляет запрос своему CCA (Центр сертификации, отвечающий за генерацию и доставку сертификатов открытых ключей владельцев карт), отправляя сообщение CardCinitReq (терминами SET) (P1).

CCA обрабатывает сообщение владельца и передает ему сертификат своего открытого ключа в сообщении CardCInitRes.

Владелец карты (точнее, конечно, его программное обеспечение), получив сообщение CardCInitRes, проверяет цифровую подпись CCA (P2). Ее

проверка эквивалентна аутентификации CCA владельцем карты. Таким образом, проверив цифровую подпись, содержащуюся в полученном от CCA сообщении, владелец карты убеждается в том, что в процессе сертификации своего открытого ключа он имеет дело с подлинным центром сертификации. Далее покупатель передает CCA номер своей карты, зашифрованный на открытом ключе CCA.

В ответ (RegFormRes) CCA передает регистрационную форму, соответствующую данной карте .

Владелец карты заполняет регистрационную форму, включая в нее сведения о себе, данные для его аутентификации (включая, например, разовый пароль предоставленный эмитентом карты) и свой открытый ключ. CCA проверяет информацию (P4) и с помощью эмитента аутентифицирует владельца карты и генерирует для него сертификат открытого ключа подписи (P6).

Сертификация продавца происходит следующим образом:

Торговая точка обращается в MCA (Центр сертификации, отвечающий за генерацию и доставку сертификатов открытых ключей торговым точкам) со специальным запросом (Me-AqCinitReq) (P7) на получение сертификата своего открытого ключа. В ответ (Me-AqCinitRes) продавец получает сертификат цифровой подписи MCA и регистрационную форму. Продавец проверяет сигнатуру ЦС (P8), отправляя ее вверх по пути сертификации до корневого центра. Также по правилам SET продавец обязан иметь два сертификата, один для подписи, а второй для шифрования симметричных сеансовых ключей. Далее требуется заполнить регистрационную форму, включая в нее аутентифицирующие продавца данные и отослать ее вместе с двумя открытыми ключами и ЭЦП, вычисленной при помощи своего закрытого ключа подписи (CertReq).

В ответ (CertRes) после проверки подлинности торговой точки с помощью его обслуживающего банка (P10) MCA генерирует сертификаты торговой точки (P12).

Аналогичным образом с помощью двухэтапной процедуры осуществляется генерация сертификата открытого ключа и для платежного шлюза. Разница состоит в том, что платежный шлюз обращается за сертификатом своего открытого ключа в PCA (Центр сертификации, отвечающий за генерацию и доставку сертификатов открытых ключей платежным шлюзам) .

Транзакция покупки

Владелец карты запрашивает сертификаты продавца и платежного шлюза сообщением PInitReq (это сообщение передается в незашифрованном виде). Продавец отвечает сообщением PInitRes, содержащим сертификаты подписи и шифрования продавца, сертификат открытого ключа шифрования сеансовых ключей платежного шлюза и глобальный идентификатор транзакции (XID), а также случайное число Chall-M. После этого ПО владельца проверяет сертификаты продавца и сертификат открытого ключа шифрования сеансовых ключей шлюза, опрашивая ЦС по обратной цепочке до первого доверенного ЦС и проверяет ЭЦП под сообщением продавца (P19,P20,P21). После подтверждения аутентичности (P23) ПО пользователя генерирует данные заказа и платежную инструкцию (P24).

Инструкция по заказу (OI) содержит в себе:

- Chall-M;
- XID;
- размер и валюту транзакции;
- идентификатор продавца;
- идентификатор набора транзакций, к которому отнесена покупка;
- номер заказа в системе магазина;
- хеш-значение от PI.

Платежная инструкция (PI) содержит в себе:

- XID;
- TranStain (хеш-значение от секрета карты S и XID);

- хеш-значение от OI;
- другая информация.

PI зашифровывается с помощью случайного сеансового ключа K1, который зашифровывается с помощью открытого ключа шифрования сеансовых ключей шлюза (PKG) и добавляется к PI. PI также содержит реквизиты карты, зашифрованные на PKG.

Торговая точка, получив сообщение PReq, проверяет сертификат владельца карты, после чего проверяет цифровую подпись владельца карты (P24,P25). Для проверки цифровой подписи торговая точка вычисляет значение хэш-функции от OI и далее, используя значение хэш-функции для PI , вычисляет общее значение H. После этого с помощью открытого ключа владельца карты дешифруется полученное из сообщения PReq значение цифровой подписи. Если дешифрованное значение совпадает с общим значением, — подпись была сделана владельцем сертификата открытого ключа владельца карты. Таким образом торговая точка аутентифицирует владельца карты.

Далее торговая точка подготавливает сообщение AuthReq (P26). В это сообщение без изменений из сообщения PReq включены зашифрованная платежная инструкция PI, зашифрованный симметричный ключ K1 и данные о реквизитах карты, а также цифровая подпись владельца карты. Кроме этих данных торговая точка формирует авторизационный запрос, содержащий информацию о размере транзакции, идентификаторе торговой точки, идентификаторе транзакции XID, случайном числе Chall-P. Эта информация подписывается ключом подписи торговой точки, зашифровывается симметричным ключом K2 сгенерированным торговой точкой по случайному закону, который в свою очередь зашифровывается открытым ключом PKG шлюза.

Платежный шлюз, получив AuthReq, расшифровывает с помощью закрытого ключа SKG оба симметричных ключа K1, и K2 а также данные о реквизитах карты, расшифровывает данные о транзакции и PI, проверяет

сертификат и подпись владельца карты (по аналогии с тем, как это делает торговая точка, для этого используется значение H содержащееся в PI) , сертификат открытого ключа подписи продавца, сертификат открытого ключа шифрования продавца, проверяет на равенство значения XID из информации о транзакции и из PI. Таким образом, платежный шлюз аутентифицирует как торговую точку, так и владельца карты (P27,28,29,P30,P31). На основании полученных данных платежный шлюз готовит стандартное сообщение для передачи его в платежную систему на авторизацию эмитента карты. Эта процедура не регламентируется SET. Достаточно будет сказать, что банковская карта имеет лимит расходования денежных средств , таким образом, если будет достигнут этот лимит транзакция будет отменена (P34).

Сеть Петри, описывающая совершение электронной транзакции по протоколу SET

На рис.1 представлена математическая модель проведения транзакции по протоколу SET, основанная на аппарате сетей Петри

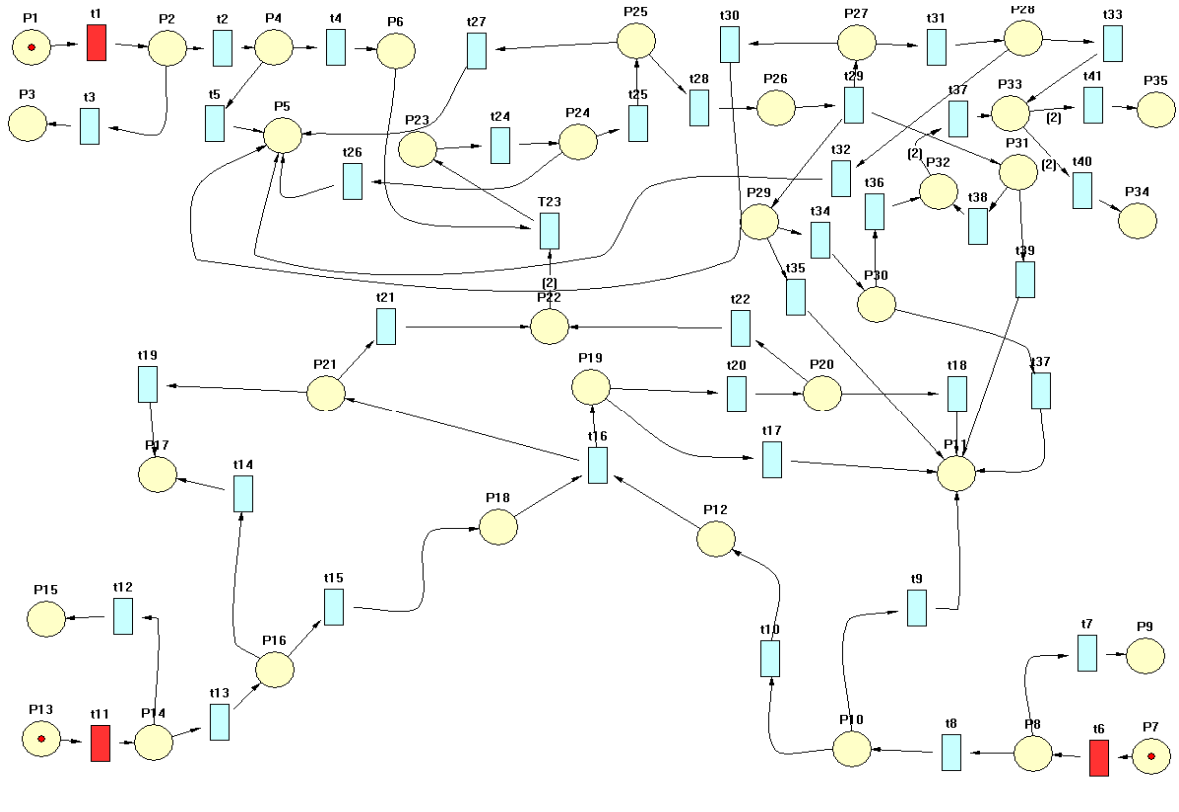

Рис. 1. Сеть Петри, описывающая процесс проведения электронного платежа по протоколу SET

Описание позиций данной сети находится в таблице 1.

Таблица 1. Описание позиций сети

Имя позиции	Смысл
P1	Отправка CardCinitReq клиентом
P2	Проверка ЭЦП CCA в сообщении CardCinitRes
P3	CCA является нарушителем
P4	Проверка RegFormRes на достоверную информацию
P5	Покупатель является нарушителем
P6	Сертификат ключа подписи покупателя получен
P7	Отправка продавцом сообщения Me-AqCinitReq
P8	Проверка ЭЦП MCA в сообщении Me-AqCinitRes
P9	MCA является нарушителем
P10	Проверка подлинности продавца центром сертификации MCA CertRes
P11	Продавец является нарушителем
P12	Получение сертификатов ключей продавца

P13	Отправка Me-AqCinitReq шлюзом
P14	Проверка ЭЦП РСА в сообщении Me-AqCinitRes
P15	РСА является нарушителем
P16	Проверка подлинности шлюза центром сертификации РСА CertRes
P17	Шлюз является нарушителем
P18	Получение сертификатов ключей шлюза
P19	Проверка сертификатов продавца в PInitRes
P20	Проверка ЭЦП продавца в PInitRes
P21	Проверка сертификата шифрования ключей шлюза в PInitRes
P22	Число прошедших аутентификацию покупателем
P23	Отправка PReq
P24	Проверка сертификата подписи покупателя продавцом
P25	Проверка ЭЦП покупателя продавцом
P26	Отправка AuthReq шлюзу
P27	Проверка сертификата подписи покупателя в AuthReq
P28	Проверка ЭЦП покупателя

P29	Проверка сертификата подписи продавца в AuthReq
P30	Проверка ЭЦП продавца
P31	Проверка сертификата шифрования продавца в AuthReq
P32	Наличие подлинных ключей продавца
P33	Число участников прошедших аутентификацию шлюзом
P34	Ответ: недостаточно средств на карте
P35	Ответ: транзакция совершена

На рисунках 2 и 3 показаны входная и выходная функции переходов данной сети

	t1	t2	t3	t4	t5	t6	t7	t8	t9	t10	t11	t12	t13	t14	t15	t16	t17	t18	t19	t20	t21	t22	t23	t24	t25	t26	t27	t28	t29	t30	t31	t32	t33	t34	t35	t36	t37	t38	t39	t40	t41
P1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P2	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P4	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P7	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P8	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P10	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P13	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P14	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P16	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
P28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0
P29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
P30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0
P31	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0
P32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0
P33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	2
P34	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0
P35	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Рис. 2. Входная функция переходов сети

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P33	P34	P35
t1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t2	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t3	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t4	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t5	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t6	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t7	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t8	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t9	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t10	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t11	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t12	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t17	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t18	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
t23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
t24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
t25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
t26	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
t27	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
t28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
t29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
t30	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
t31	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
t32	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
t34	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
t35	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t36	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
t37	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
t38	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
t39	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
t40	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
t41	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Рис. 3. Выходная функции переходов сети

Вектор, описывающий начальное состояние сети указан на рисунке 4

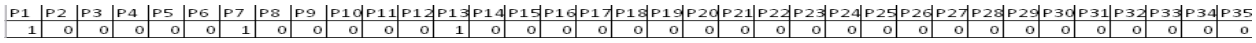

Рис. 4. Вектор начальной маркировки сети

Укажем свойства данной сети:

- Сеть потенциально живая, так как каждый из переходов может быть запущен хотя бы один раз;
- Сеть не является живой, так как в ней достижимы тупиковые маркировки;
- Сеть ограничена: максимальное число маркеров в позиции не превышает двух, следовательно не безопасная;
- Сеть не является устойчивой, так как существуют переходы, запуск которых делает невозможным срабатывание других переходов;
- Данная сеть не является консервативной: сумма ее маркеров не постоянна.

Заключение

Использование аппарата сетей Петри для представления проведения электронного платежа по протоколу SET придает данному асинхронному процессу наглядный характер. Далее при удалении некоторых дуг возможна декомпозиция данного процесса на подпроцессы. Также в дальнейшем исследовании для данной модели планируется ввести дополнительные состояния, характеризующие возможное поведение системы при введения в нее нарушителя, поведение которого описывается моделью Долева-Яо.

Библиографический список

1. Деднев М.А, Дыльнов Д.В, Иванов М.А. Защита информации в банковском деле и электронном бизнесе. – М.: Изд-во КУДИЦ-ОБРАЗ, 2004.
2. Леоненков А.В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. – М.: БХВ-Петербург, 2005.

3. Нагирняк Б. Документация к средству VisualPetri URL: http://binmount.com/programmy/visual-petri/index.php
4. Панасенко С.П., Батура В.П. Основы криптографии для экономистов. – М.: Финансы и статистика, 2005.
5. Питерсон Дж. Теория сетей Петри и моделирование систем. – М.: Мир, 1984.
6. Абдикеев М.Н. Проектирование интеллектуальных систем в экономике. – М.: Изд-во Экзамен, 2004.
7. Нагирняк Б. Документация к средству VisualPetri URL: http://binmount.com/programmy/visual-petri/index.php
8. Балюкевич Э.Л, Ковалева Л.Ф, Романников А.Н. – Дискретная математика. – М.: МЭСИ, 2007.
9. Зайцев Д.А. – Математические модели дискретных систем. – М.: Одесса: ОНАС им А.С. Попова, 2004.