ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

УДК 004.414.023

Верификация криптографических протоколов распределения ключей с использованием раскрашенных сетей Петри

Н. С. Могилевская, С. С. Колчанов
(Донской государственный технический университет)

Рассмотрена и оценена возможность применения раскрашенных сетей Петри для анализа криптографических протоколов распределения ключей на примере симметричного протокола Нидхема — Шрёдера.
Ключевые слова: *верификация протокола, формальный анализ, распределение ключей, протокол Нидхема — Шрёдера, раскрашенные сети Петри, CPN Tools.*

Введение. Одной из наиболее важных задач, которые необходимо решать при организации защиты информационной системы с помощью криптографических алгоритмов, является задача управления ключами. Очевидно, что как бы ни была сложна и разумно устроена криптосистема, некорректное обращение с ключами может значительно понизить уровень её защищённости. Под управлением ключами принято понимать информационный процесс, включающий в себя четыре основных элемента: генерацию ключей, накопление ключей, распределение ключей, процедуру их ввода и синхронизации [1, 2]. Наиболее распространённым решением задачи распределения ключей является использование специализированных криптографических протоколов.

Фактически криптографический протокол — это распределённый алгоритм, определяющий последовательность шагов, точно специфицирующих действия, которые требуются от участников для решения некоторой криптографической задачи, например, обеспечение целостности, секретности, аутентичности информации [2, 3, 4]. При анализе качества протокола необходимо обратить внимание не только на достижение желаемого результата всеми участниками протокола, но и на недопустимость проведения атак на протокол злоумышленниками. Отметим, что при анализе протокола используемые в нём криптографические алгоритмы и примитивы считаются надёжными, а анализу подвергаются сообщения, которыми обмениваются участники протокола, а именно их содержимое и порядок следования. Формальный анализ и выявление недостатков криптографических протоколов на деле оказывается весьма затруднительным. Известны факты, когда протоколы даже с небольшим количеством сообщений долгое время скрывали свои уязвимости [2, 4, 5].

Существует ряд математических аппаратов, используемых для решения задачи формального анализа протокола, например, модальные логики, конечные автоматы, спецификационные языки [2, 4, 6]. Эти подходы достаточно новые, каждый из них имеет как достоинства, так и недостатки. В обзорных работах по формальным методам анализа протоколов часто упоминается возможность верификации протоколов на основе моделирования сетями Петри, однако, исследований, посвящённых именно этому вопросу, достаточно мало, например [4, 6, 7, 8].

Цель работы. Рассмотреть и оценить возможность применения сетей Петри к верификации криптографических протоколов распределения ключей. Для достижения цели в работе с помощью раскрашенных сетей Петри для ряда криптографических протоколов построены модели. По итогам исследования моделей сделаны выводы о возможности верификации криптографических

протоколов распределения ключей с использованием раскрашенных сетей Петри. В работе исследован ряд протоколов, однако наиболее подробно рассмотрена модель выработки сеансового ключа симметричного протокола Нидхема — Шрёдера.

Протокол Нидхема — Шрёдера. Этот протокол хорошо изучен. Он получил широкую известность, так как долгое время скрывал свою уязвимость в обеспечении безопасности [2, 5]. Целью данного протокола является выработка общего сеансового ключа K_{AB} для участников протокола A и B с использованием доверенного посредника S. Говоря о доверенном посреднике для выработки ключей, мы считаем, что участники A и B уже имеют долговременные ключи для общения с ним, а кроме этого, доверяют S вырабатывать ключ для связи между участниками. Запишем протокол в виде схемы обмена сообщениями.

1. $A \to S : A,\ B,\ N_A$.
2. $S \to A : \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$.
3. $A \to B : \{K_{AB}, A\}_{K_{BS}}$.
4. $B \to A : \{N_B\}_{K_{AB}}$.
5. $A \to B : \{N_B - 1\}_{K_{AB}}$.

Здесь A, B, S — участники протокола; N_A, N_B — уникальные числовые вставки (нонсы), используемые только в одном сеансе связи; K_{AS}, K_{BS}, K_{AB} — ключи для обмена сообщениями между участниками A и S, B и S, A и B, соответственно; запись типа $\{X\}_K$ означает шифрограмму от X на ключе K; запись типа $A \to S$: X_1, X_2 означает, что участник A отправляет S сообщения X_1, X_2. Считается, что до начала протокола у участников есть договорённость об используемых криптографических алгоритмах и о порядке следования элементов в сообщениях.

Прокомментируем шаги протокола. На первом шаге пользователь A сообщает доверенному серверу S, что он намерен получить ключ для переписки с B. Во втором сообщении S генерирует ключ K_{AB} и посылает его A, в сообщении содержится также цифровая вставка N_A, по которой А узнаёт, что он получил сообщение сервера на свой запрос. На следующем шаге A отправляет B ключ K_{AB}, зашифрованный на ключе K_{BS}. Участник B доверяет этому посланию, так как оно зашифровано на ключе доверенного сервера S, а имя A, указанное в этом сообщении, говорит B, что ключ K_{AB} предназначен для общения с A. Участник B на 4-м шаге должен проверить, что отправитель сообщения $\{K_{AB}, A\}_{K_{BS}}$ действительно является A и этот участник намерен установить защищённый обмен сообщениями. Для этого он отправляет A свой нонс в зашифрованном виде. В последнем сообщении, чтобы убедить партнёра B в своей дееспособности, инициатор переговоров шифрует простое выражение, зависящее от N_B, и отправляет его A. Если все шаги протокола выполнены, то участники считают, что у них есть надёжный сеансовый ключ K_{AB}.

Процедура с использованием нонсов N_A, N_B и $N_B - 1$ служит для подтверждения участниками факта новизны, или, как принято говорить, свежести сеансового ключа K_{AB}, т. е. для подтверждения того, что указанный ключ был впервые использован в данном сеансе связи и не использовался ранее для связи этих двух участников. Основным недостатком рассмотренного протокола является то, что B не уверен в свежести ключа K_{AB}, полученного на третьем шаге. Таким образом, злоумышленник M может записать сообщения прошлых сеансов протокола и впоследствии использовать их для атаки на протокол [5].

Опишем схему протокола Нидхема — Шрёдера с атакующим злоумышленником.

1. $A \to S : A,\ B,\ N_A$.
2. $S \to A : \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$.

3. $M \to B : \{K_{AB}, A\}_{K_{BS}}$.
4. $B \to A : \{N_B\}_{K_{AB}}$.
5. $M \to A : \{N_B\}_{K'_{AB}}$.
6. $A \to B : \{N_B - 1\}_{K_{AB}}$.
7. $M \to B : \{N_B\}_{K'_{AB}}$.

На третьем шаге M отправляет старое сообщение от имени A, на четвёртом перехватывает сообщение и заменяет его на пятом шаге. Таким образом, M подменяет сообщения, адресованные B, а B верит в то, что он совместно с A в реальном времени вырабатывает новый сессионный ключ K_{AB}.

Раскрашенные сети Петри. Сети Петри — это весьма востребованный математический аппарат для моделирования динамических дискретных систем. Сеть Петри может быть задана как алгебраически, так и графически. С точки зрения алгебры, сеть Петри задаётся кортежем следующего вида $C = (P, T, I, O, \mu)$, где P, T — конечные множества позиций (состояний сети) и переходов (событий сети), I, O — множества входных и выходных функций, μ — вектор натуральных чисел, определяющий маркировку сети. Графически сеть Петри представляет собой двудольный ориентированный граф, в котором позициям соответствуют вершины, изображаемые кружками, а переходам — вершины, изображаемые чёрточками или прямоугольниками; функциям I соответствуют дуги, направленные от позиций к переходам, а функциям O — дуги, направленные от переходов к позициям. Дугами могут соединяться только вершины различных типов. Для описания динамики процессов, реализуемых в сети Петри, дополнительно вводится понятие фишки. Размещение фишек по позициям сети называется маркировкой μ. Перемещения фишек по сети представляют собой совокупность срабатываний переходов и отображают смену дискретных состояний моделируемой системы. Срабатывание перехода возможно, если имеется соответствующее переходу событие (т. н. предусловие). Выполнение события представляется фишкой в позиции, соответствующей этому условию. При запуске (срабатывании) перехода из входных позиций (предусловий) фишки удаляются, а в выходных позициях (постусловиях) — появляются. В раскрашенных сетях фишки являются элементами некоторого абстрактного типа данных, традиционно называемого цветом. Подробное описание сетей Петри хорошо представлено, например, в [9].

Идея построения моделей криптографических протоколов на основе раскрашенной сети Петри. Для построения сети Петри, отражающей работу протокола, выделим два типа объектов в моделируемом протоколе, а именно состояния и события. Под состояниями будем понимать такие сущности, как ключ, нонс, сообщение, т. е. объекты, состояние которых можно охарактеризовать одним из двух значений, например, 1 — состояние реализуется, 0 — нет. Под событиями в модели будем понимать нечто, происходящее практически мгновенно, например, отправка или получение, зашифровывание или расшифровывание сообщения. Выделенные состояния используем в качестве позиций сети, а события в модели будут представлены переходами.

Каждому участнику протокола соответствует часть построенной сети, содержащая позиции и переходы, связанные с ключами этого участника и сообщениями, которые он отправляет другим участникам. Части сети, соответствующие различным участникам протокола, между собой не пересекаются. Отметим также, что одной сущности в протоколе может соответствовать несколько позиций в сети. Как правило, эти позиции относятся к разным участникам протокола. Например, секретный ключ двух участников протокола представлен позицией у каждого из уча-

стников, а также, в зависимости от протокола, он может быть представлен дополнительно в канале связи.

Как и во всех моделях, построенных на основе сетей Петри, наличие и значение сущности в позиции определяется фишкой, а движение фишек по сети является предметом анализа сети. Для движения фишек необходимо срабатывание переходов, которое, как и наступление событий в реальной системе, определяет ход работы протокола.

В сеть может быть добавлена позиция, обозначающая успешное завершение работы протокола. Фишка в эту позицию попадает, например, если легальные участники протокола получают общий сессионный ключ. Тогда, анализируя свойство достижимости сети, при которой в этой позиции окажется нужная фишка, можно определить, приведёт ли протокол к заданной цели, а также выяснить, наступление каких событий может этому помешать.

Для проведения анализа модели криптографического протокола необходимо либо построить дерево достижимости; либо многократно запускать работу сети с различным порядком срабатывания переходов, перебирая все возможные варианты, и при этом отслеживать основные характеристики сети; либо использовать матричную теорию сетей Петри для отслеживания возможных маркировок сети [9]. Далее в работе будем использовать многократный запуск сети с помощью автоматизированных инструментов.

```
▼Declarations
  ▶Standard priorities
  ▼Standard declarations
    ▶colset UNIT
    ▼colset INT = int;
    ▶colset BOOL
    ▶colset STRING
  ▼User declarations
    ▼colset PS=string with "a".."z" and 3..3;
    ▼var Kab: PS;
    ▼var Nb_Kab, Nb1_Kab: STRING;
    ▼fun F(a)=a^"-1";
    ▼var i: INT;
    ▼var M2: STRING;
    ▼var Kas, Kbs, Kab_Kbs: STRING;
    ▼var Na, Nb, Nb1, Nb2: STRING;
```

Рис. 1. Описание переменных в терминах языка программирования CPN ML

Программный комплекс CPN Tools. Чем больше позиций и переходов содержит сеть Петри, тем сложнее её корректное построение и анализ. Для анализа моделей криптографических протоколов распределения ключей в работе использован программный комплекс CPN Tools [10], разрабатываемый группой AIS Эйндховенского университета технологий (Нидерланды) (Eindhoven University of Technology, The Netherlands). Раскрашенные сети Петри моделирующей системы CPN Tools представляют собой комбинацию графа сети Петри и языка программирования CPN ML, используемого для описания типов элементов сети. CPN Tools обладает средствами для наглядного и удобного построения и исполнения сетей Петри, обеспечивает проверку структуры конструируемых сетей, быстрое их исполнение, проведение полного или частичного анализа пространственных состояний, автоматическую проверку живости и связности. Важными характеристиками CPN Tools являются его свободное распространение, мультиплатформенность, качественная техническая поддержка и доступность документации справочного характера.

Модель протокола Нидхема — Шрёдера на основе раскрашенной сети Петри. Опишем разработанную модель подробнее. На рисунке 1 с использование языка CPN ML представлена часть описания модели, построенной в системе CPN Tools. Специальный тип данных PS был задан для описания ключей. Далее в переменных этого типа методом ran() языка CPN ML будут генерироваться случайные значения — аналоги случайных ключей. Строки описания, начинающиеся со служебного слова var, задают переменные. Описание назначения, начального значения, а также указание участников, к которым относятся эти переменные, представлены в таблице 1.

Описание переходов, используемых в построенной модели, находится в таблице 2. В левом столбце указаны названия переходов, а в правом — описания связанных с каждым из них событий. Отметим, что, так как средствами CPN ML нельзя описать алгоритм шифрования, то для имитации шифрования в работе использована конкатенация строк сообщения и ключа.

Таблица 1

Описание фишек-переменных построенной модели

Переменная	Нач. значение	Назначение	Переменная	Нач. значение	Назначение
Участник *A*			Участник *B*		
N_A	«1»	Нонс *A*	K_{BS}	«kbs»	Общий ключ *B* и *S*
K_{AS}	«kas»	Общий ключ *A* и *S*	K_{AB}	—	Сеансовый ключ
K_{AB}	—	Сеансовый ключ	N_B	«2»	Нонс *B*
N_B	—	Нонс *B*	N_{B2}	—	Нонс, полученный от *A*, после обратной операции
N_{B1}	—	Обработанный нонс *B*	N_{B1}	—	Нонс, полученный от *A*
Участник *S*			Дополнительные переменные		
K_{BS}	«kbs»	Общий ключ *B* и *S*	M_2	Канал связи между *A* и *S*	
K_{AS}	«kas»	Общий ключ *A* и *S*	$K_{AB}\_K_{BS}$, $N_B\_K_{AB}$, $N_{B1}\_K_{AB}$	Канал связи между *A* и *B*. Имя переменной совпадает с именем фишки, для которой она предназначена.	
K_{AB}	—	Сеансовый ключ	*Final!*	Конечная позиция. Содержит true в случае успешного выполнения протокола, иначе — false.	
N_A	—	Нонс *A*			

Таблица 2

Описание переходов построенной модели

Название перехода	Описание действия
T1	При появлении фишки-нонса N_A у участника *A* генерирует новый сеансовый ключ K_{AB} как случайное значение типа *PS* и сохраняет нонс для дальнейшего использования.
T2	Используя K_{BS}, шифрует сеансовый ключ K_{AB}.
T3	Собирает в одно сообщение N_A, $\{K_{AB}\}_{K_{BS}}$, K_{AB}, шифрует это сообщение ключом K_{AS} и отправляет сообщение в канал связи.
T4	Отправляет N_A к участнику *S* (инициирует работу всего протокола).
T5	Расшифровывает сообщение, извлекает из него N_A, K_{AB}, сеансовый ключ, зашифрованный ключом участника *B*, $K_{AB}\_K_{BS}$. Сохраняет K_{AB} в позиции K_{AB}, относящейся к *A*. $K_{AB}\_K_{BS}$ отправляет в канал связи с *B*.
T6	Срабатывает при получении от *B* нонса, зашифрованного сеансовым ключом. Используя сеансовый ключ из позиции *A*, расшифровывает нонс участника *B* и сохраняет его для дальнейшего использования.
T7	Получает обработанный нонс N_{B1} участника *B* и сеансовый ключ K_{AB}. Шифрует N_{B1} ключом K_{AB} и передаёт в канал связи.
T8	Принимает переменную-нонс N_B, сохраняет результат вычисления функции *F* (см. рис. 1) от значения нонса.
T9	Срабатывает при появлении в канале связи сообщения от *A*. Расшифровывает сообщение с помощью общего ключа *B* и *S* и сохраняет сеансовый ключ.
T10	Выполняет действия, обратные действиям перехода T8 с входящей фишкой и сохраняет результат.
T11	Финальный переход. Получает исходный нонс участника *B*, и нонс, полученный после обработки *A*. Отправляет в позицию *Final!* фишку true, если нонсы равны, иначе отправляет фишку false.
T12	Расшифровывает сообщение от *A* сеансовым ключом K_{AB} и сохраняет результат.
T13	Шифрует нонс участника *B* сеансовым ключом и отправляет его в канал связи.

Граф модели Петри рассматриваемого протокола, построенной в системе CPN Tools, представлен на рисунке 2. Из теории известно, что граф сети Петри задаёт алгебраическую

структуру сети однозначно и наоборот, поэтому выписывать алгебраическую структуру в явном виде не будем, чтобы не загромождать текст повтором.

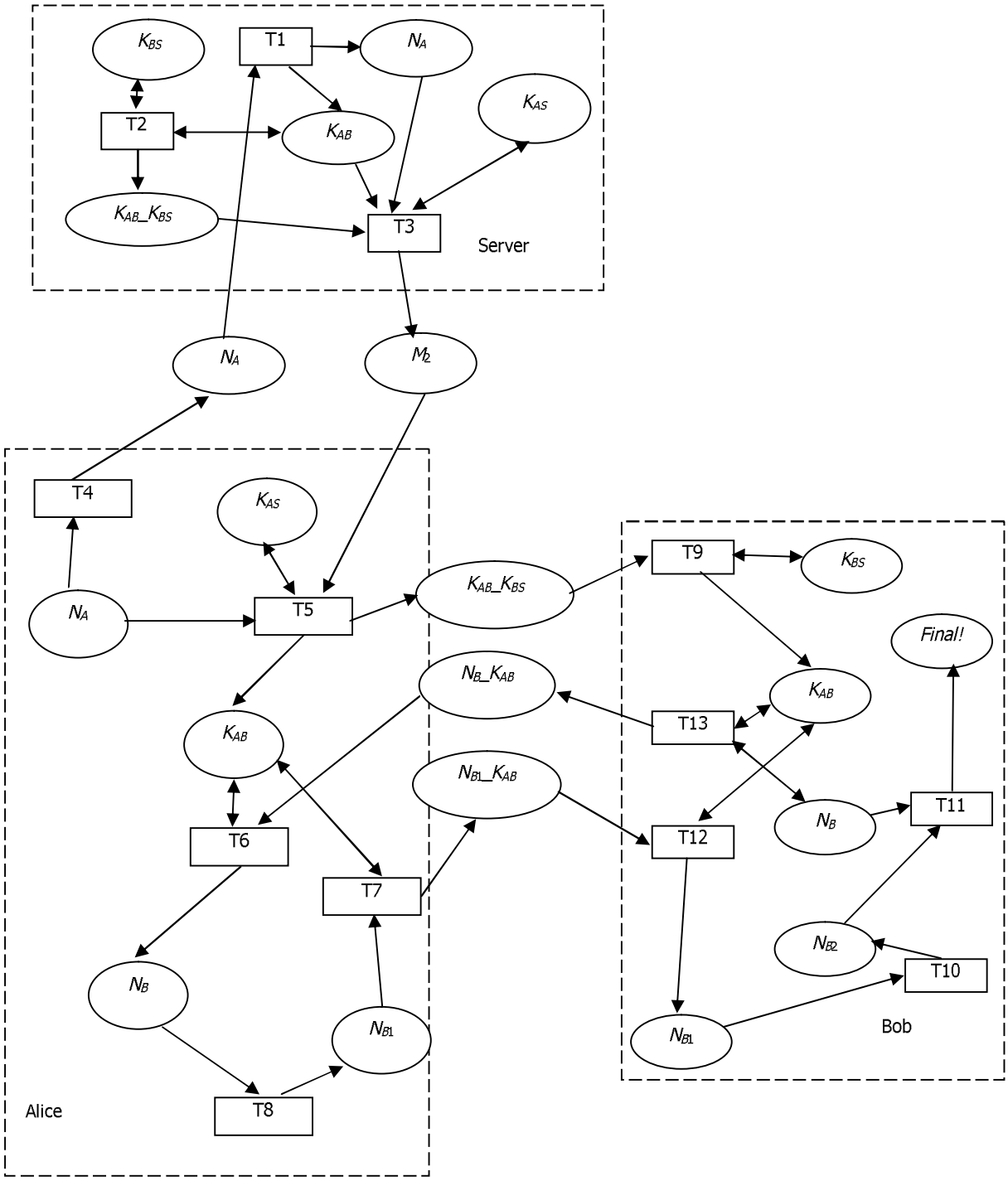

Рис. 2. Сеть Петри, моделирующая работу протокола Нидхема — Шрёдера

На графе пунктиром выделены части сети, относящиеся к различным участникам. Позиции, не вошедшие ни в какое выделение, относятся к каналу связи. Очевидно, что для построения модели злоумышленника, действующего в канале связи, необходимо «привязывать» его работу именно к этим позициям.

Результаты анализа работы модели протокола Нидхема — Шрёдера. Желаемая конечная разметка с фишкой true в позиции *Final!* и одинаковыми фишками — сеансовыми ключами в позициях K_{AB} у Алисы и Боба достигается при всех возможных вариантах последовательности срабатывания переходов, следовательно, цели протокола по результатам его исполнения достигаются. Сеть не имеет тупиковых разметок и неустойчивых переходов, следовательно, в реальной информационной системе протокол будет работать устойчиво. Во время выполнения протокола не возникает зацикливаний, количество фишек ни в одной из позиций не разрастается, следовательно, в технической реализации протокола могут быть наложены ограничения на объём памяти. Однако известная слабость протокола, связанная с возможностью использования старых сеансовых ключей, в данной модели никак себя не обнаруживает.

Результаты исследования моделей для других протоколов. В ходе данного исследования кроме модели протокола Нидхема — Шрёдера были построены модели протоколов Диффи — Хеллмана, Station-to-station и широкоротой лягушки. Модель протоколов Диффи — Хеллмана и Station-to-station выработки общего ключа, как и модель протокола Нидхема — Шрёдера, не показывает возможность реализации атаки типа «человек посередине». Однако, зная о возможности этой атаки, авторы сумели построить модели этих протоколов с учётом работы злоумышленника в сети. Полученные модели подтвердили возможность реализации такой атаки. Модель протокола широкоротой лягушки показала слабость протокола, связанную с отсутствием подтверждения получения ключа вторым участником протокола. Таким образом, в результате случайного или преднамеренного искажения ключа в канале связи между участником *A* и доверенным сервером *S* или между *S* и *B* возможна ситуация, когда участники *A* и *B* пользуются различными ключами и, как следствие, не могут читать сообщения друг друга.

Выводы по проведённым модельным экспериментам. Подведём итоги анализа моделей криптографических протоколов распространения ключей на основе сетей Петри.

К несомненным достоинствам использования сетей Петри относится их широкая распространённость. В связи с этим существует много работ, посвящённых развитию и анализу сетей, а также существуют легко доступные качественные программные средства, часто свободно распространяемые, позволяющие анализировать сети Петри в автоматическом режиме, например использованный в работе комплекс CPN Tools.

Анализ модели протокола, построенной в виде сети Петри, позволяет сделать ряд выводов, касающихся технической стороны реализации протокола. Так, достижимость финальной разметки показывает возможность достижения сетью желаемых результатов. Анализ безопасности и консервативности сети позволяет сделать вывод о возможности введения ограничений на технические средства в реальной информационной системе, например на ёмкость памяти. Рассмотрение уровня активности переходов сети позволяет выявить избыточные переходы, ситуацию взаимной блокировки в моделируемой системе, а также переходы, срабатывание которых ничем не ограничено, а, следовательно, они могут отправлять необоснованно большое количество данных в канал связи.

Сети Петри позволяют оценить возможности мошенничества легальных пользователей или работы злоумышленников в случае, когда модель криптографического протокола соединяется с моделью злоумышленника. Эта проблема исследуется в [7].

Часто исследователи к достоинствам моделей на основе сетей Петри относят их наглядность. Однако, на наш взгляд, это весьма спорное мнение, и чем больше элементов в протоколе, тем более объёмным и запутанным становится граф сети Петри.

Укажем недостатки верификации протоколов с помощью сетей. Так, при использовании сетей Петри строго не определён процесс специфицирования, то есть процесс построения графа сети по протоколу. Фактически сеть, моделирующую работу протокола и действующего в

ней злоумышленника, исследователю протокола необходимо создать вручную, что не позволяет полностью автоматизировать процесс и чревато ошибками реализации. Однако отметим, что это замечание справедливо для всех известных авторам методов математического исследования криптографических протоколов.

Модель криптографического протокола, построенная с помощью сети Петри, сама по себе малоинформативна с точки зрения возможностей злоумышленников, а также знаний и доверий легальных участников протокола и не обнаруживает многих уязвимостей. Таким образом, формальный анализ уязвимостей невозможен, допустимо лишь проверить на модели степень опасности уязвимости, найденной другим способом.

Заключение. В работе построены модели симметричных протоколов распределения ключей Нидхема — Шрёдера, Диффи — Хеллмана и широкоротой лягушки.

Результаты работы показали, что сети Петри не могут быть основным или единственным инструментом для проведения верификации криптографических протоколов. Они могут быть использованы лишь во вспомогательных целях. Во-первых, сети Петри можно применять для доказательства возможных атак и их демонстрации, во-вторых, для определения достижимости конечной маркировки, т. е. подтверждения, достигает ли протокол своей цели, в-третьих, для оценки возможности введения ограничений на технические средства в реальной информационной системе, где используется исследуемый протокол. И, наконец, для исследования возможности возникновения в протоколе «тупиков», т. е. ситуаций, когда действия участников недостаточно полно специфицированы.

Однако представляется целесообразным построение сетями Петри моделей узкого класса криптографических протоколов, в которых для подтверждения свежести ключа кроме нонсов используются и метки времени. Такая техника используется, например, в протоколах Керберос, DASS, Ньюмана — Стабблбайна [2]. Метка времени может указывать либо на время действия сеансового ключа, либо на время жизни нонса. В таком случае для моделирования нужно использовать временные сети Петри, которые отличаются от простых сетей Петри учётом времени, что позволяет моделировать не только последовательность событий, но и их привязку ко времени. Это осуществляется приданием переходам веса — продолжительности (задержки) срабатывания. Модели протоколов распределения ключей, построенные таким образом, позволят оценить безопасный диапазон времени действия ключей и нонсов.

Библиографический список

1. Основы криптографии / А. П. Алфёров [и др.]. — Москва: Гелиос АРВ, 2005. — 480 с.

2. Denning, D. E. Time stamps in Key Distribution Protocols / D. E. Denning, M. Smid // Communications of the ACM. — 1981. — V. 24. — P. 533—536.

3. Котенко, И. В. Верификация протоколов безопасности на основе комбинированного использования существующих методов и средств / И. В. Котенко, С. А. Резник, А. В. Шоров // Труды СПИИРАН. — 2009. — Вып. 8. — С. 292—310.

4. Могилевская, Н. С. Сравнение возможностей сетей Петри и BAN-логики в анализе криптографических протоколов проверки подлинности и обмена ключами / Н. С. Могилевская, С. С. Колчанов // Системный анализ, управление и обработка информации. — Ростов-на-Дону: Изд. центр ДГТУ, 2011. С. 98—101.

5. Смарт, Н. Криптография / Н. Смарт. — Москва: Техносфера, 2006. — 528 с.

6. Lin, H. Algorithms for Cryptographic Protocol Verification in Presence of Algebraic Properties: diss. for the degree of Doctor of Philosophy (Mathematics). — Clarkson University, 2009.

7. Nieh, B. Modeling and analyzing cryptographic protocols using Petri nets / B. Nieh, S. Tavares // Auscrypt'92, 1992.

8. Salah, A. Protocol verification and analysis using colored Petri nets / A. Salah, M. Khaled. — Cairo University, 2003. — P. 3—7.

9. Котов, В. Е. Сети Петри / В. Е. Котов. — Москва: Наука, 1984. — 160 с.

10. CPN Tools Homepage. Documentation. Electronic resource. Access mode: http://cpntools.org/documentation/start/ (date of access: 11.04.2011).

Материал поступил в редакцию 16.12.2011.

References

1. Osnovy` kriptografii / A. P. Alfyorov [i dr.]. — Moskva: Gelios ARV, 2005. — 480 s. — In Russian.

2. Denning, D. E. Time stamps in Key Distribution Protocols / D. E. Denning, M. Smid // Communications of the ACM. — 1981. — V. 24. — P. 533—536.

3. Kotenko, I. V. Verifikaciya protokolov bezopasnosti na osnove kombinirovannogo ispol`zovaniya sushhestvuyushhix metodov i sredstv / I. V. Kotenko, S. A. Reznik, A. V. Shorov // Trudy` SPIIRAN. — 2009. — Vy`p. 8. — S. 292—310. — In Russian.

4. Mogilevskaya, N. S. Sravnenie vozmozhnostej setej Petri i BAN-logiki v analize kriptograficheskix protokolov proverki podlinnosti i obmena klyuchami / N. S. Mogilevskaya, S. S. Kolchanov // Sistemny`j analiz, upravlenie i obrabotka informacii. — Rostov-na-Donu: Izd. centr DGTU, 2011. S. 98—101. — In Russian.

5. Smart, N. Kriptografiya / N. Smart. — Moskva: Texnosfera, 2006. — 528 s. — In Russian.

6. Lin, H. Algorithms for Cryptographic Protocol Verification in Presence of Algebraic Properties: diss. for the degree of Doctor of Philosophy (Mathematics). — Clarkson University, 2009.

7. Nieh, B. Modeling and analyzing cryptographic protocols using Petri nets / B. Nieh, S. Tavares // Auscrypt'92, 1992.

8. Salah, A. Protocol verification and analysis using colored Petri nets / A. Salah, M. Khaled. — Cairo University, 2003. — P. 3—7.

9. Kotov, V. E. Seti Petri / V. E. Kotov. — Moskva: Nauka, 1984. — 160 s. — In Russian.

10. CPN Tools Homepage. Documentation. Electronic resource. Access mode: http://cpntools.org/documentation/start/ (date of access: 11.04.2011).

VERIFICATION OF KEY MANAGEMENT CRYPTOGRAPHIC PROTOCOLS WITH COLORED PETRI NETS

N. S. Mogilevskaya, S. S. Kolchanov
(Don State Technical University)

The possibility of using colored Petri nets for the analysis of key distribution cryptographic protocols as an example of symmetric Needham—Schroeder protocol is reviewed and evaluated.

Keywords: *protocol verification, formal analysis, key management, Needham—Schroeder protocol, colored Petri nets, CPN Tools.*