А.И. Яшин
доктор технических наук, профессор, заместитель генерального директора ПАО «Интелтех»

Н.Н. Мошак
доктор технических наук, доцент, главный научный сотрудник ПАО «Интелтех»

МОДЕЛЬ ПРОТОКОЛА ДИФФИ-ХЕЛЛМАНА

АННОТАЦИЯ. В статье предлагается модель протокола Диффи-Хеллмана, которая может быть использована при проектировании защищенных сетей.

КЛЮЧЕВЫЕ СЛОВА. Мультисервисная сеть NGN, технология IntServ, протокол Диффи-Хеллмана, трафик безопасности.

Введение. Известно [1, 2], что применение механизмов защиты на фазах установления и/или поддержания сеанса связи вносит дополнительные фазовые (временные), протокольные и потоковые издержки в информационное окружение сети и приводит к ухудшению ее сетевых характеристик. В статье предложена модель протокола Диффи-Хелмана, которая может быть использована при проектировании защищенных пакетных мультисервисных сетей (МСС). Сравнительные расчеты проводятся на модели однородной МСС на технологии IntServ, которые сводятся к расчету характеристик типового незащищенного и защищенного сквозного тракта передачи и фотелекоммуникационной транспортной системы (ИТС) [2]. Указанная модель строится на базе функционального критерия эффективности системы с учетом ее архитектуры [2, 3]. Данная работа является дальнейшим развитием идей, изложенных в [1, 2, 4].

Формализация процесса генерации сеансового ключа в асимметричной криптосистеме

Использование асимметричных шифров можно свести к трем аспектам применения [5, 6]: 1) шифрование/дешифрование, при котором отправитель *i* шифрует сообщение *M* (или его сжатое отображение *H*, являющееся функцией *M*) с использованием открытого ключа P_j получателя *j*; 2) цифровая подпись $S^i(M)$, когда отправитель *i* «подписывает» сообщение *M* с помощью личного ключа S_i; 3) обмен ключами, при котором происходит обмен сеансовым ключом с применением личных ключей одной и/или обеих сторон.

Существует три метода выработки парных ключей: 1) пользователь генерирует собственные парные ключи; 2) парные ключи генерирует третья сторона; 3) парные ключи генерирует руководящий центр сертификации *CA* (Authentication Center). В данной работе мы будем рассматривать только первый метод. В общем случае механизм формирования разделяемого секрета по открытому каналу состоит в следующем. Отправитель вырабатывает разовый личный (секретный) ключ S_i (генерирует случайное число) и вычисляет открытый ключ $P_i = \alpha^{Si} (\mathrm{mod}\, p)$, который отсылает получателю. Получатель аналогичным образом вырабатывает разовый личный ключ S_j, вычисляет открытый ключ $P_j = \alpha^{S_j} (\mathrm{mod}\, p)$ и отсылает его отправителю. Оба корреспондента при этом могут вычислить общий секретный сеансовый ключ K_{ij}:

$$K_{ij} = (P_j)^{Si} = (\alpha^{Sj})^{Si} = \alpha^{SjSi} (\mathrm{mod}\, p)$$

и

$$K_{ij} = (P_i)^{Sj} = (\alpha^{Si})^{Sj} = \alpha^{SiSj} (\mathrm{mod}\, p).$$

Таким образом, любая транзакция по созданию сеансового ключа в двухключевой криптосистеме в общем случае включает в себя три фазы: а) фазу генерации общего (разделяемого) сеансового секрета K_{ij}; б) фазу взаимного обмена

общего сеансового секрета K_{ij} между корреспондентами; в) фазу аутентификации корреспондентов при создании общего сеансового секрета. Рассмотрим данные фазы подробнее.

Фаза генерации сеансового ключа K_{ij} включает в себя:

1) время, затрачиваемое на аутентификацию $t_{Pi,j}^{CAaym}$ открытых ключей пользователей P_i и P_j, получаемых по запросу из центра *CA* или без его участия — $t_{Pi,j}^{aym}$;

2) собственно время на формирование, общего секрета t_{Kij}. Время $t_{Pi,j}^{CAaym}$ в свою очередь включает время $t_{i,CA}^{запр\,Pj}$, $t_{j,CA}^{запр\,Pi}$ на запрос каждой из сторон информационного обмена сертификата партнера из центра *CA*;

3) время $t_{CA,i}^{отв\,Pj}$, $t_{CA,j}^{отв\,Pi}$ на ответ *CA* (пересылку соответствующих сертификатов) каждой из сторон;

4) время t_j^{aymCA}, t_i^{aymCA}, затрачиваемое на проверку пользователями полученных сертификатов на открытом ключе *CA*.

Если центр сертификации *CA* не участвует в процессе аутентификации, то в этом случае корреспонденты обмениваются открытыми ключами самостоятельно за время $t_{i,j}^{прд\,Pi}$ и $t_{j,i}^{прд\,Pj}$.

Фаза взаимного обмена сеансовыми ключам включает в себя время их передачи в двух направлениях между корреспондирующими парами $t_{Kij}^{прд}$.

Фаза аутентификации корреспондентов в зависимости от применяемых протоколов включает в себя:

1) время на работу протокола простой аутентификации без защиты $t_{б/з}^{aym}$ или протокола простой аутентификации с защитой $t_{с/з}^{aym}$;

2) время на работу протоколов строгой аутентификации в соответствии со стандартом X.509 с учетом одно-, двух- или трехкратном обмене аутентификационными сообщениями $t_{строг}^{aym}$.

Таким образом, транзакции по созданию сеансового ключа K_{ij} в двухключевой криптосистеме могут быть многофазовой моделью и формализоваться следующими аддитивными формами:

— при наличии центра сертификации *CA* с применением протокола простой аутентификации без защиты (с защитой) пользователей:

$$T_{Kij}^{CA1} = (t_{Pi,j}^{CAaym} + 2t_{Kij}) + 2t_{Kij}^{прд} + t_{б/з}^{aym}\,(t_{с/з}^{aym}) =$$

$$(t_{i,CA}^{запр\,Pj} + t_{j,CA}^{запр\,Pi} + t_{CA,i}^{отв\,Pj} + t_{CA,j}^{отв\,Pi} + t_j^{aymCA} +$$

$$+ t_i^{aymCA} + 2t_{Kij}) + 2t_{Kij}^{прд} + t_{б/з}^{aym}\,(t_{с/з}^{aym}); \qquad (1)$$

— при наличии центра сертификации *CA* и с применением протоколов строгой аутентификации пользователей:

$$T_{Kij}^{CA2} = (t_{Pi,j}^{CAaym} + 2t_{Kij}) + 2t_{Kij}^{прд} + t_{строг}^{aym} =$$

$$= (t_{i,CA}^{запр\,Pj} + t_{j,CA}^{запр\,Pi} + t_{CA,i}^{отв\,Pj} + t_{CA,j}^{отв\,Pi} +$$

$$+ t_j^{aymCA} + t_i^{aymCA} + 2t_{Kij}) + 2t_{Kij}^{прд} + t_{строг}^{aym}; \qquad (2)$$

— без центра сертификации *CA* с применением протокола простой аутентификации без защиты (с защитой) пользователей:

$$T_{Kij}^{1} = (t_{Pi,j}^{aym} + 2t_{Kij}) + 2t_{Kij}^{прд} + t_{б/з}^{aym}\,(t_{с/з}^{aym}) =$$

$$= t_{i,j}^{прд\,Pi} + t_{j,i}^{прд\,Pj} + 2t_{Kij} + 2t_{Kij}^{прд} + t_{б/з}^{aym}\,(t_{с/з}^{aym}); \qquad (3)$$

— без центра сертификации *CA* с применением протоколов строгой аутентификации пользователей:

$$T_{Kij}^{2} = (t_{Pi,j}^{aym} + 2t_{Kij}) + 2t_{Kij}^{прд} + t_{строг}^{aym} =$$

$$= t_{i,j}^{прд\,Pi} + t_{j,i}^{прд\,Pj} + 2t_{Kij} + 2t_{Kij}^{прд} + t_{строг}^{aym}. \qquad (4)$$

Таким образом, процесс шифрования в двухключевой криптосистеме в общем виде можно формализовать следующей аддитивной формой

$$t_{убш\_асим} = T_{Kij}^{CA1(2)}\,(T_{Kij}^{1(2)}) + t_{i,j\,убш}, \qquad (5)$$

где $t_{i,j\,убш}$ — время шифрования/дешифрования сообщения на симметричном ключе K_e на сторонах участников обмена (временем генерации ключа K_e на стороне отправителя пренебрегаем). Формализация процессов аутентификации $t_{б/з}^{aym}$ $(t_{с/з}^{aym})$, $t_{строг}^{aym}$ приведена в [3]. Здесь и далее индекс k в параметрах указывает класс трафика в терминах ATM Forum: изохронный трафик класса *B* или асинхронный трафик класса *C*.

Поток мультимедийных вызовов λ_{ij}^{multi} порождает в сети пропущенную нагрузку величины $\hat{a}_{ij}^{multi}$ (Эрл) от маршрутизатора i к маршрутизатору j

$$\hat{a}_{ij}^{multi} = N_i \lambda^{multi} t^{ses} (1 - b^{malty}), \text{ Эрл}, \quad (6)$$

где b^{malty} — величина допустимых потерь мультимедийного вызова в сети; N_i — количество мультимедийных оконечных устройств (end multimedia system, EMS), включенных в маршрутизатор i, создающих суммарную нагрузку в направлении маршрутизатора j; t^{ses}, (с) — длительность мультимедийной сессии. Суммарная величина входящего в сеть потока мультимедийных вызовов задается соответствующей матрицей $Y^{malty} = \left\| a_{ij}^{malty} \right\|$.

Каждый мультимедийный вызов порождает в сети трафик безопасности Диффи-Хеллмана величиной

$$\hat{a}_{ij}^{D-H} = N_i \lambda^{multi} t^{D-H} (1 - b^{malty}), \text{ Эрл}, \quad (7)$$

где t^{D-H}, (с) — время, необходимое для завершения транзакции протокола Диффи-Хеллмана.

При этом загрузка ρ_{ij}^{D-H} линейно-цифрового тракта сети (ЛЦТ) трафиком безопасности в сеансе связи задается выражением

$$\rho_{ij}^{D-H} = \frac{a_{ij}^{multi}}{\zeta}, \quad (9)$$

где $\zeta = \frac{t^{multi}}{t^{D-H}}$, $t^{D-H} = t_{убш\_асим}$, при его передаче внутри базовой полосы должна учитываться в общем балансе загрузки ЛЦТ.

Для однородных пакетных ИТС расчет сетевых характеристик логического соединения уровня межсетевого взаимодействия сводится к расчету параметров «типичного» для сети n-звенного составного канала [3]. Математическая модель, описывающая процесс передачи трафика классов B и C по однородному транспортному каналу в пакетной ИТС-IP-QoS, может быть представлена однолинейной многофазной СМО с ожиданием и абсолютным приоритетным обслуживанием (с дообслуживанием) речевых пакетов нагрузки по отношению к пакетам данных на каждой фазе.

На рисунке 1 представлена модель однородного логического соединения ИТС на межсетевом уровне в режиме установленного соединения. Однородный n-звенный транспортный канал представляет собой n последовательно включенных однородных межузловых ЛЦТ от источника до получателя (этот параметр учитывает качество маршрутизации информации в сети и ее топологию). На физическом уровне ЛЦТ образуют составной тракт передачи. При сделанных допущениях определим выражения для коэффициентов загрузки ρ^B, ρ^C.

Текущее значение ρ^B можно вычислить следующим образом [3].

$$\rho^B = \frac{L^B + H_{NI}}{L^B - H_{IP}} \frac{\upsilon^B}{V} a^B \eta. \quad (10)$$

Загрузка ЛЦТ трафиком данных ρ^C при условии, что процесс передачи в нем моделируется СМО $M/M/1$ с абсолютным приоритетом для речевых пакетов (с дообслуживанием), дается выражением [7]

$$\rho^C = 1 - \rho^B - \left(\frac{\frac{n\rho^B}{1-\rho^B}(L^B + H_{NI}) + n(L^C + H_{NI})}{T^C V - (L^C - H_{IP})\frac{V}{\omega^C}} \right), \quad (11)$$

где H_{NI} — заголовок уровневого примитива уровня сетевого доступа, бит; H_{IP} — заголовок уровневого примитива межсетевого уровня,

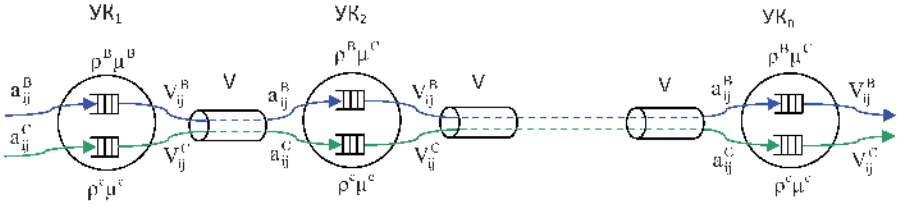

Рис. 1. Модель однородного логического соединения уровня межсетевого взаимодействия в пакетной ИТС в режиме установленного соединения

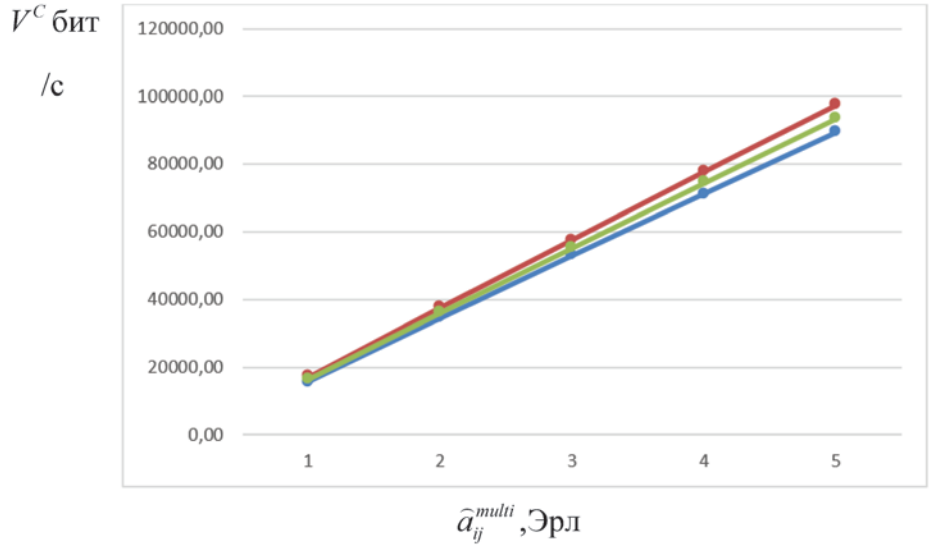

Рис. 2. Зависимость требуемой пропускной способности для передачи трафика класса *C* от величины входной речевой нагрузки в сессии:
----- без защиты, ---- с защитой (без СА), ---- с защитой (с СА)

бит; η^B — коэффициент уплотнения пауз в речевом потоке; L^B, L^C — длины протокольных блоков речи и данных на межсетевом уровне, бит; ν^B — скорость работы речевого абонента, бит/с; ω^C — скорость работы установки данных, бит/с; T^C — заданное среднее время пребывания пакета данных в ЛЦТ, с.

В предположении, что трафик безопасности обрабатывается в маршрутизаторах с приоритетом базового трафика класса *C*, загрузка ЛЦТ трафиком данных ρ^C должна увеличится на величину ρ_{ij}^{D-H}, т. е.

$$\rho^C = 1-\rho^B - \left(\frac{\frac{n\rho^B}{1-\rho^B}(L^B + H_{NI}) + n(L^C + H_{NI})}{T^C V - (L^C - H_{IP})\frac{V}{\omega^C}} \right) + \rho_{ij}^{D-H}. \quad (12)$$

Результаты расчетов параметров транспортного канала однородной ИТС представлены на графике зависимости требуемой пропускной способности ЛЦТ для передачи трафика класса *C* — V^C (бит/с) от величины входной нагрузки класса *B* (Эрл) (рис. 2). Исходные данные: $V = 128000$ бит/с, $T^C = 2c$, $n = 10$, $\omega^C = 64000$ бит/с, $\upsilon^B = 16000$ бит/с, $H_{NI} = 48$ бит, $H_{IP} = 320$ бит, $\eta^B = 0{,}497$

Анализ результатов расчетов показывает, что применение протокола Диффи-Хеллмана требует увеличения пропускной способности для трафика класса С на 4,5–9 %.

Выводы

Модели протокола Диффи-Хеллмана должны быть учтены в задачах анализа и синтеза защищенных пакетных мультисервисных сетей при расчете основных их вероятностно-временных характеристик [9,10].

ЛИТЕРАТУРА

1. **Мошак Н. Н.** Формализация и оценка процессов представления механизмов защиты в мультисервисной сети. Общий подход // Электросвязь, №3, 2012, С. 30–35.

2. **Мошак Н. Н.** Защищенные инфотелекоммуникации. Анализ и синтез: монография / Н.Н. Мошак. — СПб.: ГУАП, 2014. — 193 с.

3. **Мошак Н. Н.** Теоретические основы проектирования транспортной системы инфокоммуникационной сети: Учеб. пос. для вузов. — СПб.: Энергомашиностроение, 2006. 159 с.

4. **Мошак Н. Н.** Модели услуг аутентификации в задаче анализа инфокоммуникационной сети // Известие вузов России, Радиоэлектроника. 2007. № 5. С. 18–25.

5. **Молдовян А. А.** Введение в криптосистемы с открытым ключом / А.А. Молдовян, Н.А. Молдовян. СПб.: БХВ-Петербург, 2005. — 288 с.

6. **Молдавян А. А.** Криптография: от примитивов к синтезу алгоритмов / А.А. Молдовян, Н.А. Молдовян, М.А. Еремеев. СПб.: БХВ-Петербург, 2004. — 448 с.

7. **Клейнрок Л.** Вычислительные системы с очередями. — М.: Мир, 1979. — 600 с.

8. **Мошак Н. Н., Яшин И. Я., Давыдова Е. В.** Методы и алгоритмы анализа и синтеза пакетных мультисервисных сетей NGN // Электросвязь. № 11. 2015. — С. 46–52.

9. **Бельтов А. Г., Доскалов М. В., Кулешов И. А.** Анализ методов моделирования телекоммуникационных сетей // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2012. Т. 1. № 140. — С. 7–10.

10. **Фомин Л. А., Будко П. А., Мухин А. В., Будко Н. П.** Исследование эффективности использования ресурсов при синтезе телекоммуникационных сетей // Нейрокомпьютеры: разработка, применение. № 1, 2010. — С. 46–53.