УДК 004.05

УЛУЧШЕНИЕ СПОСОБОВ АУТЕНТИФИКАЦИИ ДЛЯ КАНАЛОВ СВЯЗИ С ОШИБКАМИ

В. Н. Никитин,
канд. техн. наук, доцент
Д. В. Юркин,
аспирант
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрен обобщенный подход к разработке и анализу криптографических протоколов с помощью вероятностно-временных методов. Показано влияние ошибок, возникающих в канале связи, на работу протоколов аутентификации.

Ключевые слова *— криптографический протокол, канал связи с ошибками, вероятностно-временные характеристики.*

Введение

Одним из основных показателей систем конфиденциальной связи, наряду со стойкостью и трудоемкостью выполнения, является эффективность использования ресурсов сети связи, обеспечивающей для корреспондентов-участников криптографического протокола своевременные предоставление доступа и передачу данных. Поэтому обеспечение высокого качества конфиденциальной связи невозможно без обеспечения заданных требований к вероятностно-временным характеристикам криптографических протоколов предоставления доступа к защищенному каналу связи и инкапсуляции данных. Наибольшей актуальностью обладает проблема идентификации и аутентификации корреспондентов в сетях широкополосного радиодоступа.

Задачи совершенствования способов аутентификации для каналов связи с ошибками

Исходя из общих требований к безопасности защищенных каналов связи можно сформулировать следующие требования к протоколам предоставления доступа [1], которые имеют в своей основе криптографические методы аутентификации:

1) сообщения протокола должны быть результатом выполнения однонаправленного преобразования, обусловленного знанием общего секрета на основе преобразования запросов и общего секрета, не компрометирующего общий секрет;

2) во избежание атаки повторения ранее переданных запросов должна быть обеспечена устойчивость к накоплению статистики передаваемых сообщений [2].

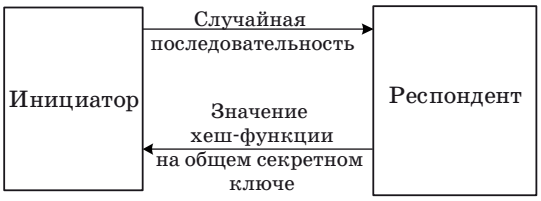
Вместе с тем, основываясь на требованиях по своевременности предоставления доступа в сетях передачи данных общего пользования [3], необходимо также обеспечить следующие вероятностно-временные требования:

- среднее время успешной аутентификации $\overline{T}$;
- вероятность успешного выполнения протокола аутентификации за допустимое время $\overline{P}(\overline{T} \le T_{exec})$.

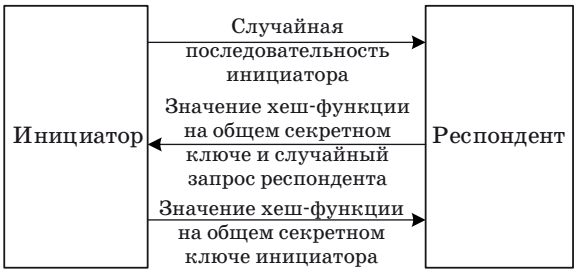
Таким образом, целью разработки является улучшение вероятностно-временных характеристик протокола аутентификации без снижения стойкости к атакам за счет сокращения числа передаваемых сообщений и уменьшения временных затрат на периодическую смену ключевой информации при применении протокола аутентификации в каналах связи с ошибками, а решаемые при этом задачи должны обеспечить достижение максимальной вероятности предоставления доступа за допустимое время в канале связи с ошибками.

Аутентификация ISO/IEC 9798 и RIPE-RACE

Известен [4–8] ряд способов аутентификации (рис. 1), использующих модель информационного



■ ***Рис. 1.*** *Способ односторонней аутентификации ISO/IEC 9798*



■ ***Рис. 2.*** *Способ двусторонней аутентификации RIPE-RACE*

взаимодействия корреспондентов типа «запрос-ответ».

В семействе стандартов ISO/IEC 9798 описан способ аутентификации, использующий модель «запрос-ответ» с применением ключевой хеш-функции, реализующий одностороннюю аутентификацию корреспондентов. Сущность способа заключается в аутентификации на основании формирования и передачи случайного запроса инициатором и вычисления респондентом ключевой хеш-функции от него с последующей передачей ее значения в ответ. Недостатком этого способа является отсутствие возможности двусторонней аутентификации корреспондентов за одну сессию протокола. Это обусловлено тем, что алгоритмы вычислений и информационного обмена сообщениями не позволяют выполнить случайные запросы инициатора и респондента в одной сессии протокола. При этом задача двусторонней аутентификации может быть решена двукратным выполнением [4] односторонней аутентификации, что потребует существенного увеличения временных затрат.

Решением задачи двусторонней аутентификации является способ RIPE-RACE [9] (рис. 2), в котором также используют ключевую хеш-функцию.

В данном способе инициатор передает случайный запрос респонденту, который, получив этот запрос, формирует свой случайный запрос, вычисляет ключевую хеш-функцию от обоих запросов и передает свой случайный запрос вместе с результатом вычисления ключевой хеш-функции. Инициатор, получив ответ респондента, вычисляет, используя секретный ключ, хеш-функцию от своего запроса, полученного запроса и идентификатора респондента и сравнивает полученное значение с принятым. В случае совпадения он вычисляет значение хеш-функции на том же ключе от обоих запросов и своего идентификатора, после чего передает его респонденту. Респондент, приняв сообщение инициатора, также вычисляет хеш-функцию от обоих запросов и сравнивает полученное значение с принятым. В случае совпадения сравниваемых величин протокол аутентификации завершен успешно.

Такой способ позволяет уменьшить число передаваемых сообщений с четырех до трех, что обеспечивает сокращение времени аутентификации для систем связи, работающих по различным каналам связи, не снижая вычислительной стойкости способа прототипа. Это повышает эффективность использования пропускной способности канала связи и снижает временные затраты на получение доступа к информационному ресурсу.

Однако рассмотренные способы имеют два недостатка:

— число передаваемых сообщений избыточно;

— криптосистемы, используемые в нем, требуют периодической смены общего секрета.

Аутентификация с использованием бесключевых хеш-функций

В рамках выбранной модели информационного взаимодействия для выполнения требуемого преобразования при аутентификации можно использовать любую условно однонаправленную функцию. Если в качестве такой функции выбрана ключевая хеш-функция [10], то заранее распределенная последовательность используется как общий секрет для вычисления однонаправленных преобразований от случайных запросов, и в целях защиты от статистических атак необходима постоянная смена общего секрета.

Однонаправленное преобразование можно реализовать с использованием другого класса функций, которым может являться класс бесключевых криптографических хеш-функций [11].

В предлагаемом способе двусторонней аутентификации корреспондентов системы связи и аутентификации при определении доступа субъекта к информационным ресурсам технических средств передачи хранения и обработки информации передается только два сообщения, вместо ключевых хеш-функций для преобразования информации используются бесключевые хеш-

функции, а общий секрет применяется в качестве аргумента хеш-функции.

Случайность однонаправленного преобразования достигается за счет конкатенации общего секрета со случайным аргументом хеш-функции, что позволяет при выборе стойкой однонаправленной функции такого класса приравнять вероятность успешной атаки на алгоритм, основанной на вычислении общего секрета, составляющего ее аргумент, к вероятности успешного обращения этой функции.

Протокол выполняется следующим образом (рис. 3). Первым сообщением передается запрос C инициатора и ответ h_R на заранее известный только легитимным корреспондентам запрос (общий секрет), а вторым — ответ h_S респондента инициатору. Причем запрос инициатора формируется путем вычисления бесключевой хеш-функции (например, алгоритмы [12, 13]) аргумента, составляющего результат вычисления $h_R = h(h_s \| C) = h(SAB \| h_s(SAB \| C)$ той же хеш-функции $h(x)$ случайного запроса и общего секрета $h_S = h(SAB \| C)$, конкатенированного со значением случайного числа, к которому добавлено само случайное число.

Ответное сообщение респондента состоит из значения бесключевой хеш-функции $h_s = h(S_{AB} \| C)$ от общего секрета и случайного запроса инициатора.

При таком информационном обмене (рис. 4) за счет уменьшения количества передаваемых сообщений сокращаются временные затраты на выполнение двусторонней аутентификации корреспондентов, а стойкость способа определяется выбором алгоритма вычисления однонаправленной бесключевой хеш-функции. Такой способ не требует периодической смены общего секрета, что позволяет сделать его долгосрочным.

Вследствие этого при работе по каналам связи с ошибками увеличивается вероятность успешного завершения протокола в заданное время, что позволяет сократить время доступа к защищенному каналу связи при заданной вероятности успешной аутентификации и улучшает доступность информационного ресурса для легитимных корреспондентов субъектов информационного обмена.

Сравнение вероятностно-временных характеристик протоколов аутентификации модели «запрос-ответ»

Приведем оценки среднего времени $\bar{T}(p_{oo})$ выполнения и вероятности успешного завершения $\bar{P}(p_{oo})$ от вероятности обнаружения ошибки в сообщениях протокола.

Согласно методике оценки вероятностно-временных характеристик криптографических протоколов [14] для рассматриваемых протоколов двусторонней аутентификации ISO/IEC 9798, SKID и предлагаемого протокола с использованием бесключевой хеш-функции при предоставлении доступа, имеем

$$\bar{T}(l, v_{form}, v_{form}, p_{oo}) = \left. \frac{\mathrm{d}}{\mathrm{d}x} \prod_{i=1}^{j} \frac{f_i^{form}(l, v_{form}, p_{oo}, x) f_i^{send}(l, v_{send}, p_{oo}, x)}{1 - f_i^{err}(l, v_{send}, p_{oo}, x) f_i^{form}(l, v_{form}, p_{oo}, x)} \right|_{x=1};$$

$$\bar{P}(l, p_{oo}, z, v_{form}, v_{send}) = 1 - \left(1 - (1 - p_{oo})^{\sum_{i=1}^{j} l_j}\right)^{\left. \mathrm{floor}\left(\frac{T_{exec}}{\bar{T}}\right) \right|_{p_{oo}=0}},$$

где l — длина кодируемого сообщения; v_{form}, v_{send} — скорости формирования и передачи сообщения соответственно; p_{oo} — вероятность обнаруженной битовой ошибки; j — число сообщений протокола.

На рис. 5, *а*, *б* показаны зависимости среднего времени и вероятности успешного завершения при $T_{exec} = 10$ с для сравниваемых протоколов применительно к сетям передачи данных стандарта IEEE 802.11 для следующих исходных данных:

скорость формирования кадра — $2 \cdot 10^9$ бит/с;

длина аргумента хеш-функции — 64 бит;

■ ***Рис. 3.*** *Информационное взаимодействие корреспондентов при двусторонней аутентификации*

Предварительные вычисления				
Распределение общего секрета				
Инициатор			Респондент	
Вычисления	Прием / передача		Прием / передача	Вычисления
$rnd(C)$ $h_S = h(S_{AB}\|C)$ $h_R = h(h_s\|C) = h(S_{AB}\|h_s(S_{AB}\|C))$				
Активные вычисления				
	C h_R	→	C h_R	$\widetilde{h}_S = \widetilde{h}(S_{AB}\|C)$ $\widetilde{h}_R = h(h_s\|C) = h(S_{AB}\|h_s(S_{AB}\|C))$ $\widetilde{h}_R = h_R$
$h_S = \widetilde{h}_S$	$\widetilde{h}_S$	←	$\widetilde{h}_S$	

■ ***Рис. 4.*** *Схема выполнения корреспондентами протокола двусторонней аутентификации*

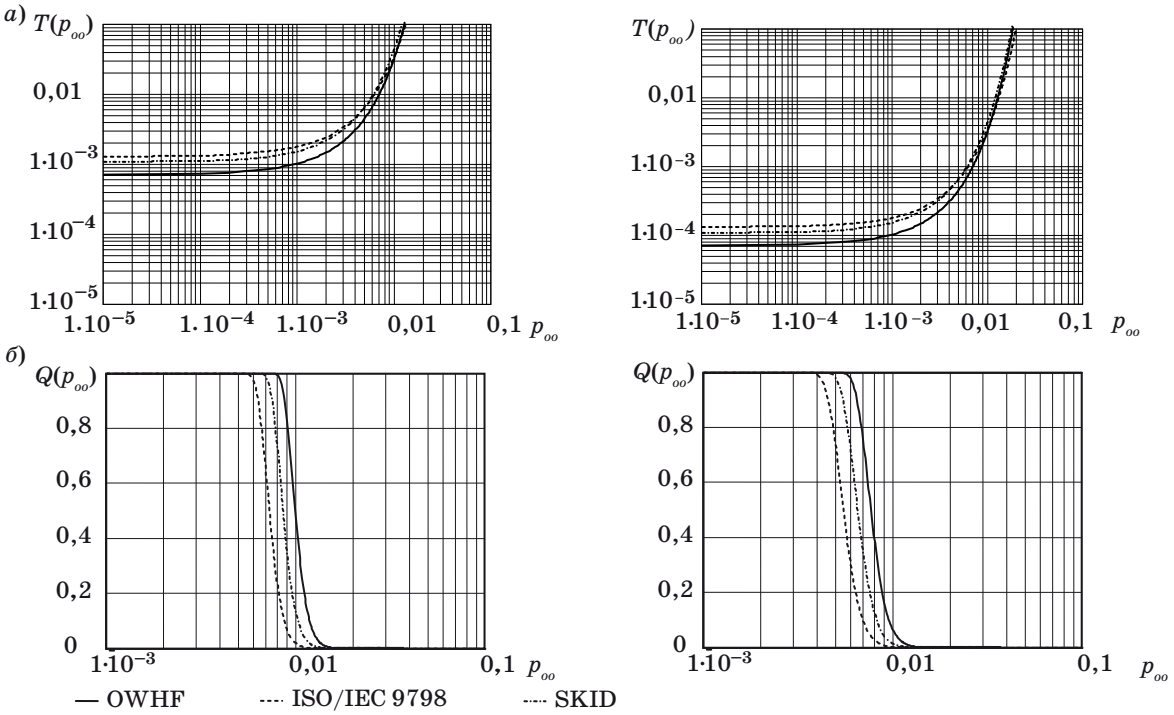
длина значения хеш-функции — 128 бит;

количество служебной информации на кадр — 224 бит.

По результатам оценки вероятностно-временных характеристик рассмотренных протоколов необходимо отметить значительное улучшение среднего времени выполнения и вероятности успешного завершения в заданное время предлагаемого способа по отношению к аналогам. Данное преимущество характеризует протокол аутентификации с использованием алгоритмов вычисления бесключевых хеш-функций как наилучший по производительности способ предоставления доступа субъекта к информационному ресурсу, эффективно работающий по каналам с высокой вероятностью ошибки.

Заключение

Анализ известных способов аутентификации модели «запрос-ответ» показывает, что они облада-



■ ***Рис. 5.*** *Зависимости среднего времени выполнения (а) и вероятности успешного завершения (б) протоколов двусторонней аутентификации: скорость передачи кадра Frame Management 10^6 бит/с (слева) и 10^7 бит/с (справа)*

ют недостатками, затрудняющими их использование в каналах низкого качества. В работе предложен способ аутентификации, позволяющий уменьшить время выполнения протокола двусторонней аутентификации, что достигается за счет сокращения числа раундов передачи сообщений до минимально возможного. Это обеспечивается вычислением бесключевой хеш-функции над конкатенацией общего секрета со случайной величиной, изменяемой при выполнении каждой последующей итерации протокола, что посредством рандомизации обеспечивает защиту от накопления статистики и атаки повторных передач сообщений. Таким образом, уникальность результата выполнения однонаправленного преобразования общего секрета достигается посредством рандомизации запроса путем добавления к аргументу вычисляемой хеш-функции случайной последовательности.

Предлагаемый способ аутентификации с использованием бесключевых хеш-функций позволяет существенно сократить время предоставления доступа в радиоканалах низкого качества.

Литература

1. **U.S.** Department of Commerce/National Bureau of Standards. Password usage. National Technical Information Service. — Virginia: Springfield, 1985. www.itl.nist.gov/fipspubs/fip112.htm (дата обращения: 10.11.08).
2. **Gong L.** Variations on the themes of message freshness and replay// The Computer Security Foundations Workshop. Geneva: IEEE Computer Society Press, 1993. P. 131–136.
3. **РД 45.128-2000.** Сети и службы передачи данных/ Министерство Российской Федерации по связи и информатизации, 2001. http://minkomsvjaz.ru/ministry/documents/959/ (дата обращения: 10.11.08).
4. **ISO/IEC 9798-1.** Information technology — Security techniques — Entity authentication mechanisms. Part 1: General model/International Organization for Standardization. — Geneva, 1991. http://www.iso.org/iso/iso_catalogue/catalogue_tc/ (дата обращения: 10.11.08).
5. **SO/IEC 9798-4.** Information technology — Security techniques — Entity authentication. Part 4: Mechanisms using a cryptographic check function/International Organization for Standardization. — Geneva, 1995. http://www.iso.org/iso/iso_catalogue/catalogue_tc/ (дата обращения: 10.11.08).
6. **ISO/IEC 9798-2.** Information technology — Security techniques — Entity authentication. Part 2: Mechanisms using symmetric encipherment algorithms/International Organization for Standardization. — Geneva, 1994. http://www.iso.org/iso/iso_catalogue/catalogue_tc/ (дата обращения: 10.11.08).
7. **ISO/IEC 9798-3.** Information technology — Security techniques — Entity authentication mechanisms. Part 3: Entity authentication using a public-key algorithm/ International Organization for Standardization. — Geneva, 1993. http://www.iso.org/iso/iso_catalogue/catalogue_tc/ (дата обращения: 10.11.08).
8. **ISO/IEC 9798-5.** Information technology — Security techniques — Entity authentication. Part 5: Mechanisms using zero knowledge techniques/International Organization for Standardization. — Geneva, 1996. http://www.iso.org/iso/iso_catalogue/catalogue_tc/ (дата обращения: 10.11.08).
9. **Bosselares A., Preneel B.** Integrity Primitives for Secure Information Systems//Final Report of RACE Integrity Primitives Evaluation RIPE-RACE 1040. N. Y.: Springer-Verlag, 1995. P. 1–12.
10. **Metzger P., Simpson W.** IP authentication using keyed MD5. 1995. http://www.ietf.org/rfc/rfc1852.txt (дата обращения: 10.11.08).
11. **Preneel B., Leuven K. U., Mercierlaan K.** Cryptographic Hash Functions: an overview// ESAT-COSIC Laboratory. Leuven, Belgium, 1994. P. 412–431.
12. **Matyas S. M., Meyer C. H., Oseas J.** Generating strong one-way functions with cryptographic algorithm// IBM Technical Disclosure Bulletin. Mar. 1985. Vol. 27. N 10A. P. 5658–5659.
13. **Miyaguchi S., Ohta K., Iwata M.** 128-bit hash function (N-hash)//NTT Review. Nov. 1990. Vol. 2. N 6. P. 128–132.
14. **Nikitin V., Yurkin D., Chilamkurti N.** The influence of the cryptographic protocols on the quality of the radio transmission// ICUMT. St.-Petersburg, Russia, Nov. 2009. P. 1–5.