УДК 004.05

ПОВЫШЕНИЕ ЗАЩИТЫ ПРОТОКОЛОВ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ОТ АТАК ВТОРЖЕНИЯ В СЕРЕДИНУ КАНАЛА СВЯЗИ

В. Н. Никитин[a]***,*** *канд. техн. наук, доцент*
М. М. Ковцур[a]***,*** *соискатель*
Д. В. Юркин[a]***,*** *канд. техн. наук, доцент*
[a]*Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Санкт-Петербург, РФ*

Постановка проблемы: *алгоритм Диффи — Хеллмана широко применяется во многих протоколах распределения ключей, в том числе в протоколах IP-телефонии. Однако протокол является неустойчивым к атаке активного нарушителя в канал связи, что приводит к компрометации выработанного ключевого материала. Целью работы является разработка методов повышения защиты протоколов распределения ключей, основой которых является протокол Диффи — Хеллмана.* ***Методы:*** *исследованы особенности распространения пакетов между узлами глобальной сети Интернет в разных городах при использовании нескольких провайдеров связи.* ***Результаты:*** *выполнены оценки вероятностей совпадения пар и троек маршрутов в глобальной сети между разными городами при подключении через нескольких операторов связи. Изложен подход к повышению защищенности протоколов распределения ключей при помощи параллельной передачи сообщений по независимым каналам связи для случая, когда корреспонденты не имеют общего секрета. В работе приведены методы обнаружения и снижения влияния действий нарушителя на работу протоколов распределения ключей. Представлены оценки вероятностей успешной атаки, обнаружения атаки активного нарушителя, успешной генерации общего секрета.* ***Практическая значимость:*** *результаты исследований позволяют повысить безопасность существующих протоколов распределения ключей.*

Ключевые слова *— криптографические протоколы, протоколы распределения ключей.*

Введение

Схема распределения ключей Диффи — Хеллмана, лежащая в основе многих криптографических протоколов, получила широкое распространение среди схем распределения ключей между корреспондентами и позволяет корреспондентам выработать общий секретный ключ для симметричного шифрования данных. Данная схема является основой безопасного распределения ключевого материала для протоколов обеспечения безопасности IP-телефонии ZRTP [1–3], MIKEY [4], DTLS [5] и др.

Вместе с тем схема Диффи — Хеллмана может быть полностью компрометирована активным нарушителем при реализации атаки вторжения в середину канала связи. Поэтому при реализации алгоритма распределения ключей необходимо обеспечить подлинность сообщений протокола [6]. С этой целью схему Диффи — Хеллмана обычно реализуют в защищенном канале передачи данных, для которого невозможно выполнить подмену передаваемых сообщений [7, 8]. При этом для аутентификации передаваемых сообщений, как правило, используют цифровые сертификаты.

Однако в случае необходимости выработки общего секретного ключа корреспондентов, которые не имеют общего доверенного удостоверяющего центра, требование обеспечения аутентичности сообщений протокола Диффи — Хеллмана не обеспечивается.

Способ обнаружения атак вторжения в середину протокола Диффи — Хеллмана

В настоящее время наличие у одного корреспондента двух и более подключений к транспортной сети является обычным явлением. Для обнаружения нарушителя предлагается модифицировать протокол распределения ключей так, чтобы выполнять обмен сообщениями с использованием нескольких каналов связи одновременно.

Рассмотрим ситуацию, когда корреспонденты, имеющие по два или более подключений к транспортной сети, пытаются установить защищенное соединение IP-телефонии без участия посредников. Подключения выполняются через разных операторов связи с различными публичными IP-адресами для каждого из сетевых подключений. Для организации защищенного соединения корреспонденты обмениваются IP-адресами, создавая два или более виртуальных каналов.

При выполнении протокола, как показано на рис. 1, передаются одинаковые сообщения по каждому из каналов. При этом респондент, получив сообщения, проверяет их на совпадение. Если обнаружено несовпадение — имеет место атака MITM (Man in the Middle) в одном из каналов [9, 10].

Респондент отвечает, отправляя по двум каналам связи ответные сообщения. Инициатор получает сообщения и выполняет аналогичную проверку. Если сообщения одинаковые, значит либо отсутствует активный нарушитель в двух

■ ***Рис. 1.*** Обмен сообщениями по двум каналам связи

каналах связи, либо присутствует активное воздействие одного нарушителя на оба канала связи одновременно.

Очевидно, что подготовка к атаке вторжения требует значительных ресурсов нарушителя, поэтому вероятность вторжения в несколько каналов меньше, чем вероятность вторжения в один из каналов. Наиболее критична ситуация, когда трассы используемых каналов в некоторых узлах сходятся, поскольку нарушитель, атакуя такой узел, может воздействовать на все каналы.

При модификациях протокола распределения ключей, заключающихся в использовании нескольких каналов связи, возрастает актуальность оценки вероятностей успешной атаки MITM, обнаружения атаки MITM и успешной генерации общего секрета.

Реализация протокола Диффи — Хеллмана по двум независимым каналам

Введем вероятность $P_{\text{у.а1}}$ того, что нарушитель выполняет атаку MITM в одном из каналов. Под успешной атакой на модифицированный протокол будем понимать событие успешной атаки MITM в каждом из каналов. Это возможно в том случае, когда один и тот же нарушитель контролирует используемые каналы и может выполнять синхронную модификацию сообщений в каждом из каналов. Тогда вероятность успешной атаки $P_{\text{у.а2}}$ соответствует модификации сообщений в двух каналах связи одновременно:

$$P_{\text{у.а2}}=(P_{\text{у.а1}})^2.$$

Обнаружение нарушителя определим как событие несовпадения сообщений протокола в различных каналах. Вероятность обнаружения нарушителя $P_{\text{о.н2}}$ для двухканальной схемы соответствует вероятности нахождения нарушителя в одном канале связи при отсутствии в другом:

$$P_{\text{о.н2}}=2(1-P_{\text{у.а1}})\,P_{\text{у.а1}}.$$

Успешная выработка ключа возможна только в случае необнаружения нарушителя ни в одном канале связи. Однако совпадение сообщений возможно и в том случае, когда нарушитель присутствует в обоих каналах и производит согласованную подмену сообщений. Поскольку эти события несовместны, вероятность успешной выработки ключа равна разности вероятностей отсутствия и присутствия нарушителя в обоих каналах:

$$P_{\text{у.к2}}=(1-P_{\text{у.а1}})^2-P_{\text{у.а2}}^2=1-2P_{\text{у.а1}}.$$

Следует отметить, что необходимость синхронной модификации сообщений в двух каналах связи требует от нарушителя дополнительных ресурсов по сравнению с модификацией сообщений по отдельности в каждом из каналов связи.

Реализация протокола Диффи — Хеллмана по трем независимым каналам

Пусть по трем каналам связи будут передаваться одинаковые сообщения схемы Диффи — Хеллмана, тогда результатом работы протокола является одно из нескольких событий:

1) все принятые сообщения совпадают;

2) одно сообщение отличается от других;

3) все сообщения разные.

В первом случае протокол не обнаруживает нарушителя.

Во втором случае протокол позволяет обнаружить нарушителя без определения атакованного канала или определить такой канал и исключить его при формировании ключа.

В третьем случае атака обнаруживается, но атакованные каналы не идентифицируются.

Поэтому возможно выделить два режима работы протокола — с обнаружением и исключением нарушителя.

При работе в режиме *обнаружения* нарушителя протокол завершается с ошибкой, уведомляя пользователя о наличии нарушителя в канале связи.

В случае работы в режиме *исключения* нарушителя при обнаружении отличий в одном из сообщений протокол уведомляет о наличии нарушителя в конкретном канале связи, при этом он продолжает работу и учитывает сообщения лишь из тех каналов связи, где не обнаружен нарушитель. Вероятность правильного исключения на-

рушителя $P_{\text{пр.и}}$ для трехканального протокола соответствует событию нахождения нарушителя в одном из каналов связи при его отсутствии в двух других:

$$P_{\text{пр.и}} = 3P_{\text{у.а1}}(1-P_{\text{у.а1}})^2.$$

При воздействии нарушителя одновременно на два канала связи из трех возможных, с синхронной модификацией сообщений механизм исключения может вызвать некорректное определение канала с нарушителем, что приведет к ошибочному выбору надежных каналов. Это позволит нарушителю успешно выполнить обмен ключами с корреспондентами, осуществив атаку MITM.

Вероятность ошибочного исключения соответствует вероятности события, что нарушителем выполнена одновременная подмена сообщений сразу в двух каналах связи:

$$P_{\text{ош.и}} = 3P_{\text{у.а1}}^2(1-P_{\text{у.а1}}).$$

Расчет вероятностей трехканального протокола в режиме обнаружения нарушителя.

Вероятность успешной атаки $P_{\text{у.а3\_о.н}}$ соответствует вероятности того, что нарушитель перехватил и выполнил модификацию сообщений сразу в трех каналах одновременно:

$$P_{\text{у.а3\_о.н}} = P_{\text{н3к}} = (P_{\text{у.а1}})^3.$$

Определим вероятность обнаружения нарушителя $P_{\text{о.н3\_о.н}}$.

Вероятность наличия нарушителя в одном из каналов при отсутствии нарушителя в двух других каналах связи

$$P_{\text{нар1к\_нет\_нар23к}} = 3(1-P_{\text{у.а1}})^2 P_{\text{у.а1}}.$$

Вероятность наличия нарушителя в двух каналах при отсутствии нарушителя в третьем равна

$$P_{\text{нет\_нар1к\_нар23к}} = 3(1-P_{\text{у.а1}})P_{\text{у.а1}}^2;$$

$$P_{\text{о.н3\_о.н}} = P_{\text{нар1к\_нет\_нар23к}} + P_{\text{нет\_нар1к\_нар23к}} = 3(1-P_{\text{у.а1}})^2 P_{\text{у.а1}} + 3(1-P_{\text{у.а1}})P_{\text{у.а1}}^2.$$

Вероятность успешного формирования общего ключа $P_{\text{у.к3\_о.н}}$ для трехканального протокола в режиме обнаружения нарушителя соответствует вероятности отсутствия нарушителя в трех каналах связи. Следовательно:

$$P_{\text{у.к3\_о.н}} = P_{\text{нет\_нар}}^3 = (1-P_{\text{у.а1}})^3.$$

Расчет вероятностей трехканального протокола в режиме исключения нарушителя.

Вероятность успешной атаки $P_{\text{у.а3\_и.н}}$ соответствует вероятности события перехвата и модификации сообщений нарушителем в двух или трех каналах связи одновременно, которая равна

$$P_{\text{у.а3\_и.н}} = (P_{\text{у.а1}})^3 + 3(1-P_{\text{у.а1}})\,P_{\text{у.а1}}^2.$$

Вероятность обнаружения нарушителя $P_{\text{о.н3\_и.н}}$ соответствует вероятности нахождения нарушителя в одном канале связи при отсутствии нарушителя в двух других каналах связи.

Вероятность наличия нарушителя в одном из каналов связи при отсутствии нарушителя в двух других каналах связи будет иметь вид

$$P_{\text{о.н3\_и.н}} = 3(1-P_{\text{у.а1}})^2 P_{\text{у.а1}}.$$

Вероятность успешного формирования общего ключа $P_{\text{у.к3\_и.н}}$ соответствует вероятности отсутствия нарушителя в двух или трех каналах связи. Следовательно:

$$P_{\text{у.к3\_и.н}} = (1-P_{\text{у.а1}})^3 + 3(1-P_{\text{у.а1}})^2 P_{\text{у.а1}}.$$

Зависимости рассмотренных вероятностей от вероятности успешной подмены сообщений в одном из каналов связи для исходного протокола и модифицированного в двух- и трехканальном варианте показаны на рис. 2, *а—в*.

Экспериментальная оценка вероятности совпадения виртуальных каналов транспортной сети

Структура глобальной транспортной сети описана в различных источниках [11]. Маршрутизация пакетов осуществляется динамическими протоколами и зависит от многих параметров [12]. Предположим, что структура глобальной сети является случайной.

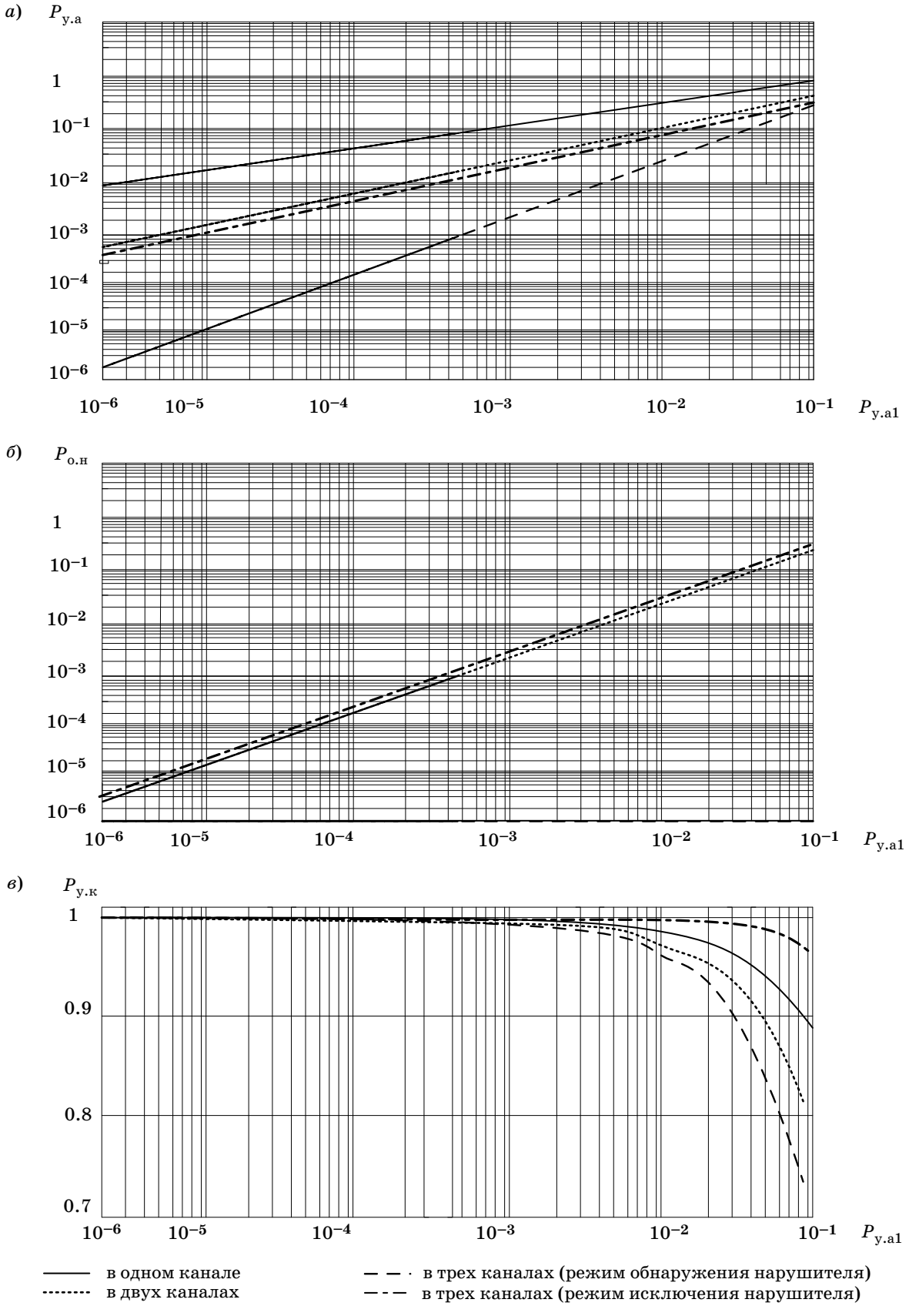
Максимальное число групп независимых маршрутов W определяется соотношением

$$W = \prod_{i=0}^{nS-i} (N_S - i)(N_d - i)(n_S!)^{-1},$$

где N_s — число начальных точек маршрутов; N_d — число удаленных точек маршрутов; n_s — количество независимых маршрутов, сравниваемых для анализа числа совпадений.

Для трассировки маршрутов от начальной до удаленной точки использовались программно-аппаратные средства, состав и конфигурация которых остается за рамками данной работы. В результате сравнения маршрутов было получено число пар и троек непересекающихся маршрутов, а также количество маршрутов, на которых встречались общие точки. При сравнении троек маршрутов дополнительно оценивалось число маршрутов без общих точек, а также число троек маршрутов с одной, двумя или тремя общими точками. Итоговые данные эксперимента представлены в таблице.

Из общего числа пар маршрутов 2478 в 122 обнаружены совпадения. Таким образом, только



■ ***Рис. 2.*** Вероятность: *а* — успешной атаки MITM; *б* — обнаружения нарушителя; *в* — успешной выработки ключа

■ Число независимых пар и троек маршрутов

Страна	Город	Число точек в городе	Для пар маршрутов/для троек маршрутов			
			общее число маршрутов	число маршрутов без общих точек	число маршрутов с общей точкой	совпадение маршрутов, %
Россия	Барнаул	3	60/60	59/57	1/3	1,67/5,00
Россия	Москва	3	60/60	60/60	0/0	0,00/0,00
Россия	Новосибирск	3	60/60	60/60	0/0	0,00/0,00
Германия	Берлин	3	60/60	57/51	3/9	5,00/15,00
Германия	Мюнхен	3	60/60	60/60	0/0	0,00/0,00
США	Нью-Йорк	4	120/240	119/234	1/6	0,83/2,50
США	Эдисон	3	60/60	59/57	1/3	1,67/5,00
Австралия	Сидней	3	60/60	58/57	2/3	3,33/5,00
Австралия	Мельбурн	5	200/600	157/116	43/484	21,5/81,07
Россия	Санкт-Петербург	12	1320/13200	1320/13200	0/0	0,00/0,00
США	Даллас	3	60/60	51/33	9/27	15,00/45,00
Япония	Фукуока	3	60/60	34/0	26/60	43,33/100,00
Япония	Токио-Чийода	7	420/2100	384/1576	36/524	8,57/24,95
Всего				2478/15561	122/1119	

4,4 % из всех возможных пар имели общие точки. В результате эксперимента не обнаружено городов, к которым все подходящие пары маршрутов имели бы общую точку. Использование двух или трех каналов связи, предоставляемых разными операторами связи, позволяет с большой вероятностью организовать независимые каналы, не имеющие общих точек, и существенно уменьшить вероятность необнаруженного вторжения.

Заключение

Модификация протокола для работы по нескольким независимым каналам существенно уменьшает вероятность успешной атаки MITM. Эффективность защиты возрастает с увеличением числа независимых каналов.

Исследования показывают, что при подключении корреспондентов к нескольким операторам связи независимые двойки и тройки маршрутов имеются всегда. Вероятность успешного формирования общего ключа в многоканальной схеме с обнаружением нарушителя уменьшается незначительно. В схеме с исключением нарушителя данная вероятность увеличивается, но при использовании трасс большой протяженности возможно совпадение узлов прохождения маршрутов, что может снизить эффективность работы модифицированного протокола.

Литература

1. **Ковцур М. М., Никитин В. Н., Юркин Д. В.** Оценка вероятностно-временных характеристик защищенной IP-телефонии // Защита информации. Инсайд. 2012. № 4. С. 64–71.
2. **Ковцур М. М., Никитин В. Н., Винель А. В.** Исследование вероятностно-временных характеристик протокола распределения ключей защищенной IP-телефонии // Информационно-управляющие системы. 2013. № 1. С. 54–63.
3. **RFC 6189.** ZRTP: Media Path Key Agreement for Unicast Secure. 2011. http://tools.ietf.org/html/rfc6189 (дата обращения: 20.10.2013).
4. **RFC 3830.** MIKEY: Multimedia Internet KEYing. August, 2004. http://tools.ietf.org/html/rfc3830 (дата обращения: 25.10.2013).
5. **RFC 5764.** Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP). http://tools.ietf.org/html/rfc5764 (дата обращения: 29.10.2013).

6. **Коржик В. И., Просихин В. П.** Основы криптографии: учеб. пособие по специальности 210403 «Защищенные телекоммуникационные системы связи». – СПб.: Линк, 2008. – 256 с.
7. **Яковлев В. А., Коржик В. И., Бакаев М. В.** Протоколы формирования ключа на основе каналов связи с шумом в условиях активного перехвата с использованием экстракторов // Проблемы информационной безопасности. Компьютерные системы. 2006. № 1. С. 51–67.
8. **Патент 2183348,** Российская Федерация G06F12/14, H04L9/32. Способ аутентификации объектов / Молдовян А. А., Молдовян Н. А., Никитин В. Н., Фокин А. О. – № 2000119274/09; заявл. 19.07.2000; опубл. 10.06.2002, Бюл. № 6. – 9 с.
9. **Макарова О. С.** Методика формирования требований по обеспечению информационной безопасности сети IP-телефонии от угроз среднестатистического «хакера» // Докл. Томского государственного университета систем управления и радиоэлектроники. 2012. № 1. С. 51–67.
10. **Говор Т. А.** Обеспечение безопасности современных VOIP-сетей // Радиопромышленность. 2011. № 4. С. 37–43.
11. **Перфильев Ю. Ю.** Российское интернет-пространство: развитие и структура. – М.: Гардарики, 2003. – 272 с.
12. **Левин В., Дякив Д.** SLA в России пять лет спустя // Журнал сетевых решений LAN. 2013. № 09. С. 35–39.

UDC 004.05

Enhancement of Security of Key Distribution Protocols Against Intruder Attacks in the Middle of a Communication Channel

Nikitin V. N.[a], PhD, Tech., Associate Professor, vnikitin@rdnet.ru
Kovtsur M. M.[a], Post-Graduate Student, maxkovzur@mail.ru
Yurkin D. V.[a], PhD, Tech., Associate Professor, dvyurkin@yandex.ru
[a]Bonch-Bruevich Saint-Petersburg State University of Telecommunications, 22 – 1, Bol'shevikov St., 193232, Saint-Petersburg, Russian Federation

Purpose: Diffie — Hellman algorithm is widely used in many key distribution protocols including IP-telephony protocols. However the protocol is unstable against an active intruder attack in a communication channel resulting in discrediting generated key material. The goal of the paper is to develop methods to enhance security of key distribution protocols based on Diffie — Hellman protocol. **Methods:** There have been studied particularities of package distribution between different nodes of the global Internet web in different cities using several communication providers. **Results:** There have been carried out estimates of probability of matching pairs and triplets of paths in the global network between different cities using several communication operators. There has been stipulated an approach to enhance security of key distribution protocols by means of distribute message transmission through two or three independent channels in the case when correspondents do not have a shared secret. The paper has revealed techniques to detect and to decrease influence of intruder actions against performance of key distribution protocols. There have been presented estimates of probabilities of a successful attack, an active intruder attack detection and successful generation of a shared secret. **Practical relevance:** The research results allow to enhance security of the existing key distribution protocols.

Keywords — Cryptographic Protocols, Key Distribution Protocols.

References

1. Kovtsur M. M., Nikitin V. N., Iurkin D. V. Estimation of the Time-Probabilistic Characteristics of Secure IP-Telephony. *Zashchita informatsii. Insaid*, 2012, vol. 46, no. 4, pp. 64–71 (In Russian).
2. Kovtsur M. M., Nikitin V. N., Vinel' A. V. Analysis of the Time-Probabilistic Characteristics of Key Agreement Protocol for Secure IP-Telephony. *Informatsionno-upravliaiushchie sistemy*, 2013, vol. 62, no. 1, pp. 54–63 (In Russian).
3. *RFC 6189. ZRTP: Media Path Key Agreement for Unicast Secure.* 2011. Available at: http://tools.ietf.org/html/rfc6189 (accessed 20 October 2013).
4. *RFC 3830. MIKEY: Multimedia Internet KEYing.* 2004. Available at: http://tools.ietf.org/html/rfc3830 (accessed 25 October 2013).
5. *RFC 5764. Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP).* 2010. Available at: http://tools.ietf.org/html/rfc5764 (accessed 29 October 2013).
6. Korzhik V. I., Prosikhin V. P. *Osnovy kriptografii* [Foundations of Cryptography]. Saint-Petersburg, Link Publ., 2008. 256 p. (In Russian).
7. Iakovlev V. A., Korzhik V. I., Bakaev M. V. Protocols for Generating a Key Based Communication Channel with Noise Pickup Conditions Using Active Extractors. *Problemy informatsionnoi bezopasnosti. Komp'iuternye sistemy*, 2006, no. 1, pp. 51–67 (In Russian).
8. Moldovian A. A., Moldovian N. A., Nikitin V. N., Fokin A. O. *Sposob autentifikatsii ob»ektov* [Object's Authentication Method]. Patent Russian Federation, no. 2000119274/09, 2002.
9. Makarova O. S. Formation Technique Requirements for Information Security IP-Telephony Network from Threats Average "Hacker". *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniia i radioelektroniki*, 2012, vol. 25, no. 1, pp. 64–68 (In Russian).
10. Govor T. A. Securing VOIP-Modern Networks. *Radiopromyshlennost'*, 2011, no. 4, pp. 37–43 (In Russian).
11. Perfil'ev Iu. Iu. *Rossiiskoe internet-prostranstvo: razvitie i struktura* [Russian Internet Space: the Development and Structure]. Moskow, Gardariki Publ., 2003. 272 p. (In Russian).
12. Levin V., Diakiv D. SLA in Russia Five Years Later. *Zhurnal setevykh reshenii LAN*, 2013, no. 9, pp. 35–39 (In Russian).