УДК 004.05

ИССЛЕДОВАНИЕ ПУТЕЙ СОВЕРШЕНСТВОВАНИЯ ПРОТОКОЛОВ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ В ЗАЩИЩЕННОЙ IP-ТЕЛЕФОНИИ

Ковцур М.М.

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, e-mail: maxkovzur@mail.ru

Представлена математическая модель активного нарушителя, учитывающая возможность этого нарушителя реализовать атаку «человек посередине» на протокол распределения ключей и позволяющая рассчитать вероятность успешной атаки, нацеленной на несанкционированный доступ к информации, в зависимости от значений вероятностей промежуточных атак. Изложен учитывающий особенности криптографического протокола ZRTP подход к повышению защищенности протоколов распределения ключей посредством параллельной передачи специализированных сообщений по независимым каналам связи для случая, когда корреспонденты не имеют общего секрета. Выполнена оценка достигнутого повышения безопасности. Описан способ улучшения временных характеристик криптографического протокола ZRTP, позволяющий сократить время успешного выполнения протокола при работе по каналам связи с большими задержками, а также произведена оценка среднего времени успешного выполнения при реализации этого способа.

Ключевые слова: криптографические протоколы, протоколы распределения ключей, повышение безопасности

INVESTIGATION OF THE WAYS OF IMPROVING OF THE KEY AGREEMENT PROTOCOLS IN THE SECURE IP-TELEPHONY

Kovtsur M.M.

The Bonch-Bruevich St. Petersburg State University of Telecommunications, Saint-Petersburg, e-mail: maxkovzur@mail.ru

A mathematical model of the active intruder, taking into account the intruder's possibility to realize attack man in the middle (MITM) for key distribution protocol, is described. Model allows to calculate the probability of a successful attack, aimed at unauthorized access to information (NSD), depending on the probabilities of intermediate attacks. Way of applying methods of security improvement for key agreement protocols for ZRTP is described. Increase of security is achieved through parallel transmission of specialized messages over the independent communication channels and applied when correspondents have no shared secret. Way of improving the time characteristics of a cryptographic protocol ZRTP, which allows to reduce the time of the execution of the protocol while working on the communication channels with large delays is described.

Keywords: cryptographic protocols, key agreement protocol, security improvement

Протоколы распределения ключей (ПРК) используются в безопасной IP-телефонии для согласования параметров защищенного соединения, а также для формирования общего секрета между корреспондентами для этого соединения. Протоколы распределения ключевого материала исследованы с точки зрения обеспечения безопасности и возможных атак, однако достаточно слабо изучены способы улучшения их характеристик. В роли показателей качества протоколов предлагается использовать вероятность успешной атаки несанкционированного доступа (НСД) на систему безопасной IP-телефонии, а также среднее время успешного выполнения протокола распределения ключей для установления защищенного соединения.

Существующие модели [1, 3, 4, 5, 9, 10] не учитывают атаку «человек посередине» (MITM) на ПРК и не позволяют определить вероятность успешной атаки НСД на систему защищенной IP-телефонии, работающую по схеме корреспондент-корреспондент. Вследствие этого целесообразно разработать такую модель нарушителя, которая позволила бы решить данную задачу.

Математическая модель нарушителя

Для построения математической модели нарушителя выполнен анализ угроз и их источников. Используя уязвимости, активный нарушитель может выполнять комбинацию атак, которая может привести к достижению НСД.

В качестве основных возможных атак активного нарушителя выделены:

1. Перебор пароля для доступа к управлению оборудованием оператора или пользователя.
2. Организация проксирования или перенаправления всего или части трафика любым доступным способом.
3. Выполнение атаки MITM на ПРК и другие протоколы безопасной IP-телефонии.
4. Атака на шифр – перебор ключа к перехваченному медиатрафику.
5. Установка закладки, модификация программного обеспечения (ПО) терминала пользователя.
6. Установка дополнительного оборудования на узле оператора связи.

7. Изменение настроек терминала пользователя для частичного отключения безопасности.

8. Перехват авторизационных данных для управления терминалом пользователя за счет прослушивания трафика управления шлюзом.

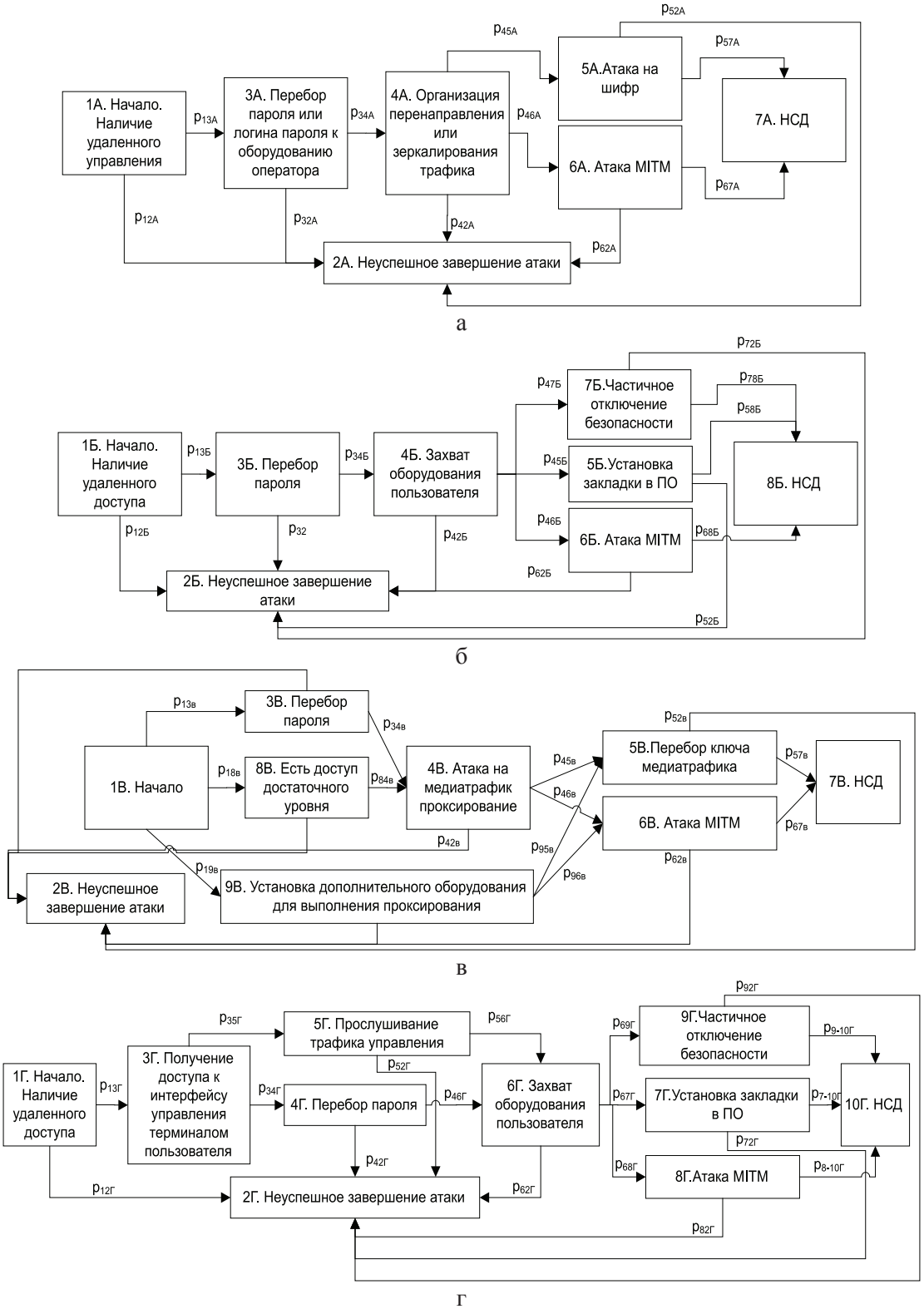


Рис. 1. Возможный алгоритм действий при выполнении:
а – захвата оборудования оператора внешним нарушителем; б – захват терминала пользователя внешним нарушителем; в – захвата оборудования оператора внутренним нарушителем; г – захват терминала пользователя внутренним нарушителем

При разработке модели нарушителя введено допущение, что если субъект атаки находится в одной сети с объектом атаки, то такой нарушитель является внутренним. В противном случае он является внешним. Тогда промежуточными целями нарушителей с точки зрения получения НСД являются:

а) захват оборудования оператора внешним нарушителем;

б) захват терминала пользователя внешним нарушителем;

в) захват оборудования оператора внутренним нарушителем;

г) захват терминала пользователя внутренним нарушителем.

Разработка модели начинается с анализа алгоритмов действий нарушителя по каждой из перечисленных целей. Алгоритмы возможных действий нарушителя представлены на рис. 1.

Используя возможные алгоритмы действий нарушителя, составлены вероятностные графы, представленные на рис. 2.

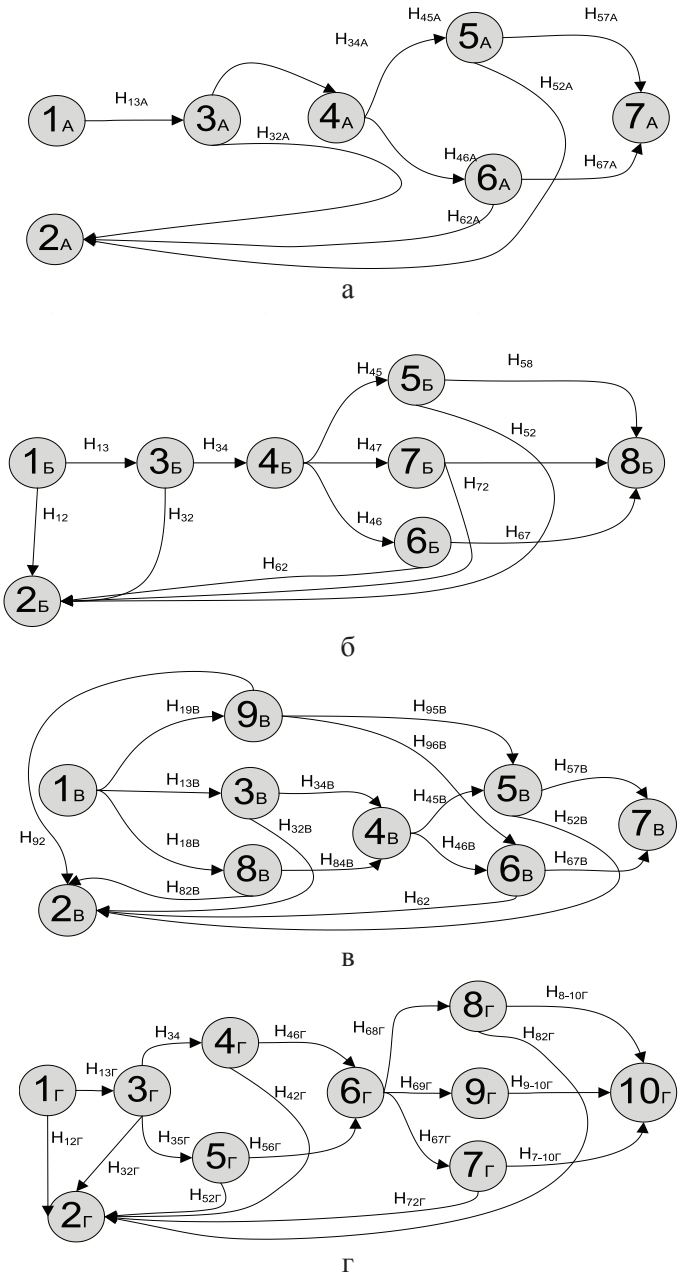


Рис. 2. Вероятностный граф:
а – захват оборудования оператора внешним нарушителем; б – захват терминала пользователя внешним нарушителем; в – захват оборудования оператора внутренним нарушителем; г – захват терминала пользователя внутренним нарушителем

По каждому графу выделена ветвь, соответствующая успешному выполнению атаки НСД и составлена производящая функция $H(x)$ этой ветви.

Для каждого из рассматриваемых графов в соответствии с методикой, приведенной в [6], приведены $P_{\text{НСД}} = H(x = 1)$:

$$P_{\text{нсдА}} = p_{13\text{А}} p_{34\text{А}} (p_{45\text{А}} p_{57\text{А}} + p_{46\text{А}} p_{67\text{А}}); \quad (1)$$

$$P_{\text{нсдБ}} = p_{13\text{Б}} p_{34\text{Б}} (p_{45\text{Б}} p_{58\text{Б}} + p_{46\text{Б}} p_{68\text{Б}} + p_{47\text{Б}} p_{78\text{Б}}); \quad (2)$$

$$P_{\text{нсдВ}} = ((p_{13\text{В}} p_{34\text{В}} + p_{18\text{В}} p_{84\text{В}}) p_{45\text{В}} + p_{19\text{В}} p_{95\text{В}}) p_{57B} + ((p_{13\text{В}} p_{34\text{В}} + p_{18\text{В}} p_{84\text{В}}) p_{46\text{В}} + p_{19\text{В}} p_{96\text{В}}) p_{67\text{В}}; \quad (3)$$

$$P_{\text{нсдГ}} = p_{13\text{Г}} (p_{34\text{Г}} p_{46\text{Г}} + p_{35\text{Г}} p_{56\text{Г}}) (p_{67\text{Г}} p_{7-10\text{Г}} + p_{68\text{Г}} p_{8\text{-}10\text{Г}} + p_{69\text{Г}} p_{9\text{-}10\text{Г}}), \quad (4)$$

где p_{ijX} – вероятность перехода из вершины i в вершину j соответствующего графа.

$$P_{\text{нсд}} = \max \{P_{\text{нсдА}}, P_{\text{нсдБ}}, P_{\text{нсдВ}}, P_{\text{нсдГ}}\}. \quad (5)$$

Очевидно, в случае установления соединения в сценарии корреспондент-корреспондент без сервера и при отсутствии предварительно распределенного ключевого материала сам пользователь является наиболее заинтересованным лицом для повышения безопасности и снижения $P_{\text{НСД}}$. При этом пользователь может применять VoIP терминал, поддерживающий функцию отключения удаленного управления, что приведет к $p_{13\text{Б}} = 0$, $p_{13\text{Г}} = 0$, и, как следствие, $P_{\text{НСДБ}} = 0$, $P_{\text{НСДГ}} = 0$.

Однако пользователь не может оказывать влияние на вероятности *pijA*, *pijB*. В зависимости от промежуточных целей нарушителя можно выделить несколько частных моделей нарушителей, представленных в табл. 1.

Следует заметить, что $p_{57\text{А}}$, $p_{57\text{В}}$ зависят от применяемого алгоритма шифрования. Существующие рекомендации SRTP предусматривают использование алгоритма AES с ключом 128 или 256 бит. Взлом такого алгоритма является крайне маловероятным [2]. По этой причине наиболее вероятным будет выбор атаки MITM на ПРК со стороны нарушителя. Следовательно, можно ввести допущение, что вероятность выбора атаки на шифр $p_{45\text{А}} = 0$, $p_{45\text{В}} = 0$, а вероятность выбора атаки MITM $p_{46\text{А}} = 1$, $p_{46\text{В}} = 1$.

Тогда верятность успешной атаки НСД будет иметь вид

$$P_{\text{нсд}} = \max \{P_{\text{нсдА}}, P_{\text{нсдБ}}, P_{\text{нсдВ}}, P_{\text{нсдГ}}\}, \quad (6)$$

и тогда

$$P_{\text{нсдА}} = p_{13\text{А}} p_{34\text{А}} p_{46\text{А}} p_{67\text{А}}; \quad (7)$$

$$P_{\text{нсдБ}} = 0;$$

$$P_{\text{нсдВ}} = ((p_{13\text{В}} p_{34\text{В}} + p_{18\text{В}} p_{84\text{В}}) p_{46\text{В}} + p_{19\text{В}} p_{96\text{В}}) p_{67\text{В}}; \quad (8)$$

$$P_{\text{нсдГ}} = 0.$$

В зависимости от промежуточных целей и возможностей можно также выделить несколько нарушителей (В1, В2, В3, А4), представленных в табл. 1.

Подставив значения p_{ijX} из табл. 1 в формулы (7), (8), получаем:

$$P_{\text{нсдВ1}} = p_{34\text{В}} p_{67\text{В}}; \quad (9)$$

$$P_{\text{нсдВ2}} = p_{84\text{В}} p_{67\text{В}}; \quad (10)$$

$$P_{\text{нсдВ3}} = p_{67\text{В}}; \quad (11)$$

$$P_{\text{нсдА4}} = p_{34\text{А}} p_{67\text{А}}; \quad (12)$$

$$P_{\text{НСД}} = \max \{P_{\text{нсдВ1}}, P_{\text{нсдВ2}}, P_{\text{нсдВ3}}, P_{\text{нсдА4}}\}. \quad (13)$$

Очевидно, что $P_{\text{нсдВ3}}$ больше или равна $P_{\text{нсдВ1}}$, $P_{\text{нсдВ2}}$, $P_{\text{нсдА4}}$. Следовательно, $P_{НСД}$ будет определяться величиной $p_{67\text{В}}$, которая будет соответствовать атаке НСД внутреннего нарушителя на узле оператора связи посредством установки дополнительного оборудования для организации MITM.

Повышение безопасности ПРК ZRTP

Протокол ZRTP детально описан в [8, 13] и имеет встроенный механизм защиты от MITM, однако он не устойчив против атаки активного нарушителя, владеющего технологией синтеза голоса, а также требует от пользователей дополнительных действий для вербальной проверки аутентификационной строки SaS.

Можно выделить два подхода по применению способа повышения безопасности ПРК [7] применительно к ZRTP:

- Использование дополнительных каналов связи для автоматической проверки аутентификационной строки SaS;
- Использование дополнительных каналов связи для передачи сообщений протокола.

Первый подход позволяет сократить общий объем информации, передаваемой по каналам связи, однако при его использовании наличие MITM может быть определено только по завершению формирования ключа, а также будет требовать дополнительного времени. Использование же второго подхода позволяет определить нарушителя во время выполнения протокола ZRTP.

Таблица 1

Вероятность атак в зависимости от целей нарушителя

Обозначение и определение вероятности	Возможные значения вероятностей	Цели нарушителей			
		B1) Атака внутреннего нарушителя через захват оборудования оператора за счет перебора пароля и организация MITM	B2) Атака внутреннего нарушителя при наличии у него доступа на оборудование путем организации MITM	B3) Атака внутреннего нарушителя через установку дополнительного оборудования на узле оператора путем организации MITM	A4) Атака внешнего нарушителя через захват оборудования оператора за счет перебора пароля и организация MITM
p_{13B} – вероятность выбора атаки «перебор пароля для доступа к оборудованию оператора»	0..1	1	0	0	–
p_{18B} – вероятность наличия доступа достаточного уровня на оборудование оператора	$0...1 – p_{13B}$	0	1	0	–
p_{19B} – вероятность наличия у нарушителя возможности установки дополнительного оборудования на узле оператора связи для выполнения атаки	$0...1 – p_{18B} – p_{13B}$	0	0	1	–
p_{34A},p_{34B} – вероятность успешного завершения атаки «перебор пароля для доступа к управлением оборудования оператора»	0...1	0...1	–	–	0...1
p_{84B} – вероятность использования нарушителем имеющегося доступа достаточного уровня на оборудование оператора	0...1	–	0...1	–	-
p_{46A}, p_{46B} – вероятность выбора «атаки MITM на ПРК и другие протоколы безопасной IP-телефонии»	$0...1 – p_{45A}$ $0...1 – p_{45B}$	1	1	–	1
p_{67A},p_{67B} – вероятность успешного завершения «атаки MITM на ПРК и другие протоколы безопасной IP-телефонии»	0...1	0...1	0...1	0...1	0...1
p_{96B} – вероятность выбора «атаки MITM на ПРК и другие протоколы безопасной IP-телефонии»	$0...1 – p_{95B}$	–	–	1	–
p_{13A} – вероятность наличия возможности удаленного подключения к оборудованию оператора	0 или 1	–	–	–	1

Рассмотрим детальнее первый подход повышения безопасности ZRTP, реализуемый за счет внедрения механизма автоматической проверки SaS в протокол с использованием дополнительного канала связи. В качестве такого канала связи может выступать SMS, пакет с данными, отправленный по сети с пакетной коммутацией, и т.д. Схема взаимодействия корреспондентов показана на рис. 3, а.

Корреспонденты обмениваются сообщениями протокола ZRTP по первому каналу связи и успешно завершают протокол. По окончанию обмена каждый корреспондент локально вычисляет значение символьной аутентификационной строки SaS в соответствии с [13]. Далее корреспонденты обмениваются вычисленными значениями SaS по второму независимому каналу связи. Если полученное по каналу связи значение SaS совпадает с локально вычисленным значением, значит, либо отсутствует нарушитель в обоих каналах связи, либо один и тот же нарушитель контролирует оба канала связи. В соответствии с [7] вероятность успешной атаки MITM в этом случае будет иметь вид

$$P_{\text{УА2\_SaS}} = (P_{H1K})^{2б}, \qquad (14)$$

где P_{H1K} – вероятность наличия в одном канале связи нарушителя, способного выполнить атаку MITM.

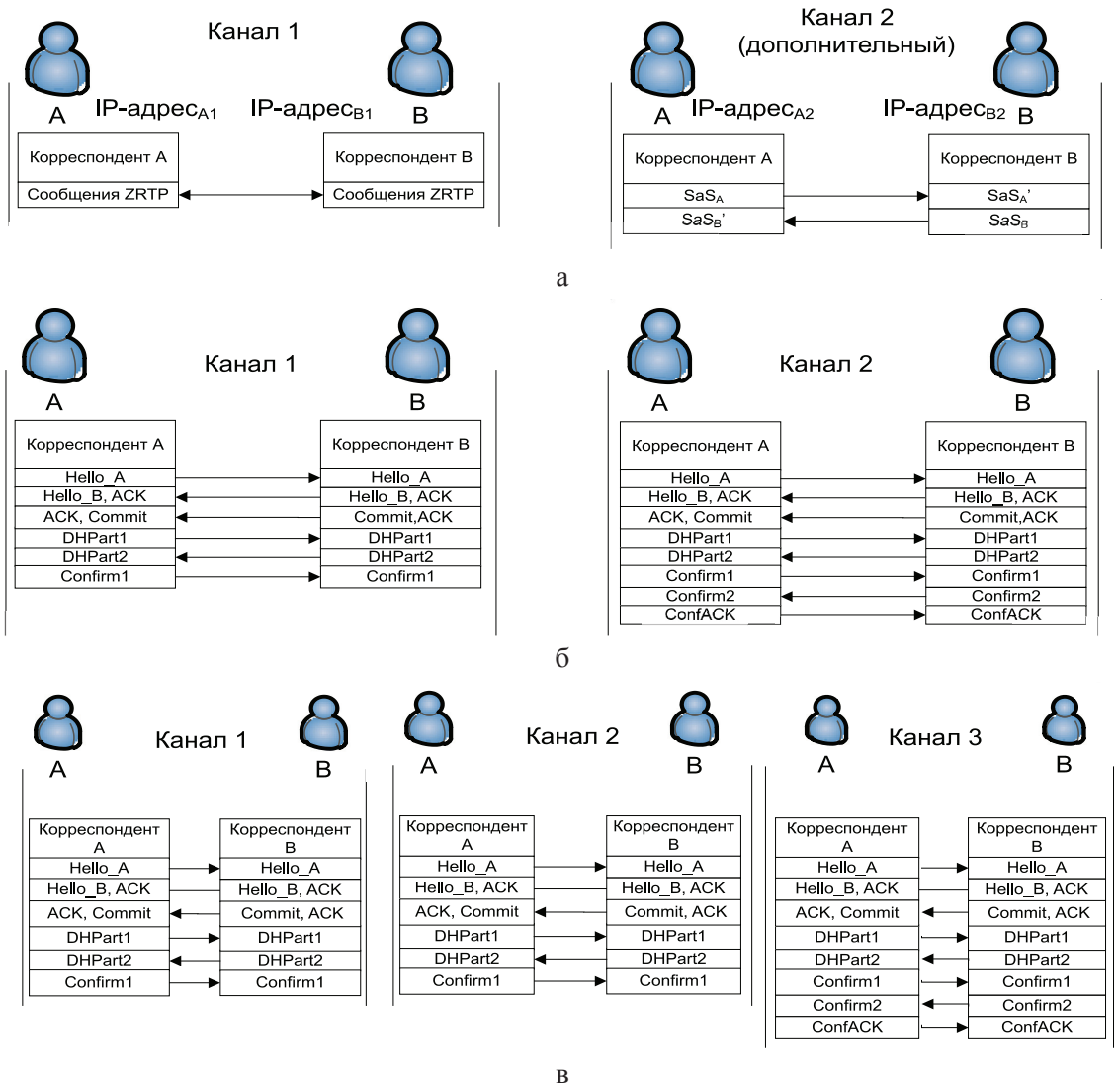


Рис. 3. Вариант взаимодействия корреспондентов при использовании: а – механизма автоматической проверки SaS для протокола ZRTP; б – двухканального режима ZRTP; в – трехканального режима ZRTP

В качестве второго пути повышения безопасности ZRTP можно использовать предлагаемый в [7] подход – добавить в ZRTP двухканальный и трехканальный режимы, обмен сообщениями при которых представлен на рис. 3, б и в соответственно.

Для двухканального режима протокола вероятность успешной атаки MITM $P_{УА2}$ будет иметь вид

$$P_{УА2} = (P_{H1K})^2. \quad (15)$$

Для трехканального режима протокола вероятность успешной атаки MITM $P_{УА3}$ будет иметь вид

$$P_{УА3} = (P_{H1K})^3. \quad (16)$$

Для оценки эффективности способа повышения безопасности вычислим выигрыш $B_{НСД}$ как

$$B_{НСД} = P_{нсд\_мод}/P_{нсд\_ориг}, \quad (17)$$

где $P_{нсд\_мод}$ – вероятность успешной атаки НСД на модифицированный протокол; $P_{нсд\_ориг}$ – вероятность успешной атаки НСД на оригинальный протокол.

Выигрыш показывает, насколько изменилась – увеличилась или уменьшилась вероятность успешной атаки НСД модифицированного ПРК по сравнению с исходным.

Для двухканального режима протокола с автоматической проверкой SaS

$$B_{2K\_SaS} = P_{нсд\_2K\_SaS}/P_{нсд\_ориг} = p_{67B\_2K\_SaS}/p_{67B\_ориг} = (P_{H1K})^2/P_{H1K} = P_{H1K}. \quad (18)$$

Для двухканального режима протокола ZRTP:

$$В_{2К} = P_{нсд\_2К}/P_{нсд\_ориг} = p_{67В\_2К}/p_{67В\_ориг} = (P_{H1K})^2/P_{H1K} = P_{H1K}. \quad (19)$$

Для трехканального режима протокола ZRTP:

$$В_{3К} = P_{нсд\_3К}/P_{нсд\_ориг} = p_{67В\_3К}/p_{67В\_ориг} = (P_{H1K})^3/P_{H1K} = P_{H1K}^2. \quad (20)$$

Так как $P_{H1K} <= 1$, то во всех случаях наблюдается уменьшение вероятности успеха НСД, что эквивалентно повышению уровня безопасности. Насколько видно, предложенный способ позволяет уменьшить вероятность успешной атаки НСД в $1/P_{H1K}$ раз для двухканального режима протокола по сравнению с оригинальным протоколом ZRTP и в $1/(P_{H1K})^2$ раз для трехканального режима протокола. Так, при $P_{H1K} = 0{,}01$ получаем выигрыш в уменьшении вероятности успешной атаки НСД в 100 раз для двухканального протокола и в 10000 раз для трехканального протокола.

Улучшение временных характеристик ПРК ZRTP

Сценарий обмена сообщениями в оригинальном протоколе ZRTP [8] представлен на рис. 3, б, канал 2. Обмен сообщениями включает четыре фазы, каждая из которых имеет свое назначение.

Протокол выполняется после организации соединения между корреспондентами, что влияет на время установления защищенного голосового канала связи. Информация о размерах сообщений протокола ZRTP, а также оценка среднего времени успешного выполнения этого протокола при задержках $d = 50$–300 мс и при различных значениях вероятности битовой ошибки p_0 в канале связи представлены в [6]. Среднее время успешного выполнения протокола превышает 1,5 с при работе по каналам с задержками более 200 мс. В соответствии с [12] кодек G.711 обеспечивает высокое качество, MoS ≥ 4, для $d <= 300$ мс. Поэтому целесообразным является уменьшение среднего времени выполнения протокола для соблюдения норм [11] даже при работе по каналам с задержками до 300 мс. Поэтому необходимо разработать способ улучшения временных характеристик криптографического протокола ZRTP.

Предлагаемый способ уменьшения среднего времени успешного выполнения состоит в отказе от использования механизма выбора инициатора и респондента, а также в объединении информационных данных о поддерживаемых криптографических наборах ZRTP и информационных блоков протокола Диффи – Хелмана.

Инициатором в этом случае предлагается выбирать корреспондента, который первым отправил сообщение *DHPart*1. Если сообщение отправили оба корреспондента, то инициатор определяется по значению *hvi* согласно [13].

Обмен сообщениями протокола в модификации, а также соответствующий вероятностный граф приведены на рис. 4 а и б.

У вероятностного графа выделена ветвь, соответствующая успешному выполнению ZRTP, определена производящая функция $H_{ZRTP\_MOD}(x)$ этой ветви и вычислено среднее время успешного выполнения ZRTP $T_{СР\_ZZRTP\_MOD}$ при различных значениях d задержки в канале связи и при различных значениях битовой ошибки p_0 в канале связи:

$$T_{CP\_ZRTP\_MOD} = \frac{dH_{ZRTP\_MOD}(x)}{dx}(x=1); \quad (21)$$

$$T_{CP\_ZRTP\_OLD} = \frac{dH_{ZRTP\_OLD}(x)}{dx}(x=1), \quad (22)$$

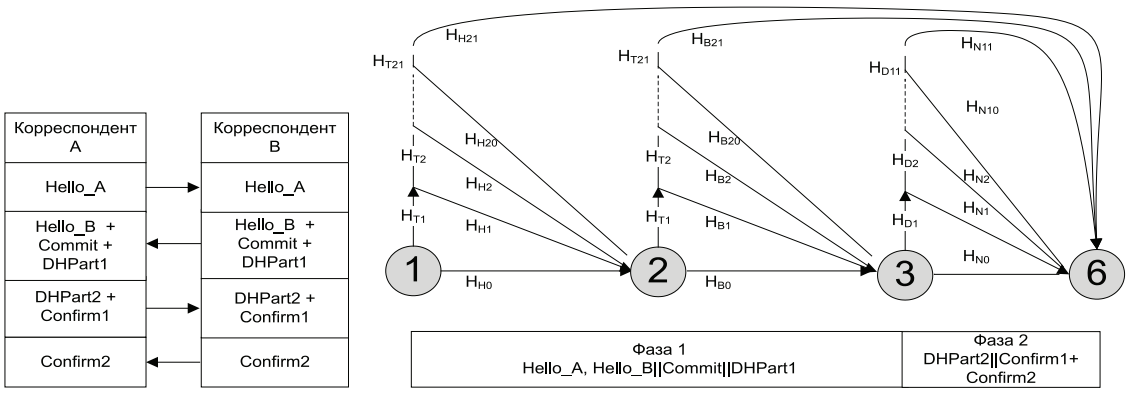
где $H_{ZRTP\_MOD}(x)$ – производящая функция ветви успешного завершения модификации ZRTP; $H_{ZRTP\_OLD}(x)$ – производящая функция ветви успешного завершения оригинального ZRTP.

График $T_{СР\_ZZRTP\_MOD}$ от p_0 для модификации ZRTP приведен на рис. 4.

Выигрыш $В_В$ по сравнению с исходным протоколом определяется по формуле (23) и составляет от 39,42 % до 48,34 % (табл. 2).

$$В_В = (T_{ZRTP\_OLD} - T_{ZRTP\_MOD})/T_{ZRTP\_OLD}, \quad (23)$$

где $T_{СР\_ZRTP\_OLD}$ – среднее время выполнения исходного протокола ZRTP; $T_{СР\_ZRTP\_MOD}$ – среднее время выполнения модифицированного протокола.



а б

Рис. 4. Модификация протокола:
а – сценарий обмена сообщениями; б – вероятностный граф

Таблица 2

Оценка выигрыша среднего времени успешного завершения модифицированного ZRTP

Задержка	50 мс			150 мс			300 мс			400 мс		
p_0	10^{-5}	$5{\cdot}10^{-5}$	10^{-4}	10^{-5}	$5{\cdot}10^{-5}$	10^{-4}	10^{-5}	$5{\cdot}10^{-5}$	10^{-4}	10^{-5}	$5{\cdot}10^{-5}$	10^{-4}
$T_{CP\_ZRTP\_OLD}$, с	0,52	0,58	0,7	1,3	1,38	1,5	2,5	2,59	2,7	3,32	3,38	3,51
$T_{CP\_ZRTP\_MOD}$, с	0,315	0,36	0,451	0,715	0,76	0,851	1,315	1,36	1,45	1,715	1,76	1,851
Выигрыш, с	0,205	0,22	0,249	0,585	0,62	0,649	1,185	1,23	1,24	1,605	1,62	1,659
B_B, Выигрыш, %	39,42	37,93	35,57	45,00	44,93	43,27	47,40	47,49	46,26	48,34	47,93	47,26

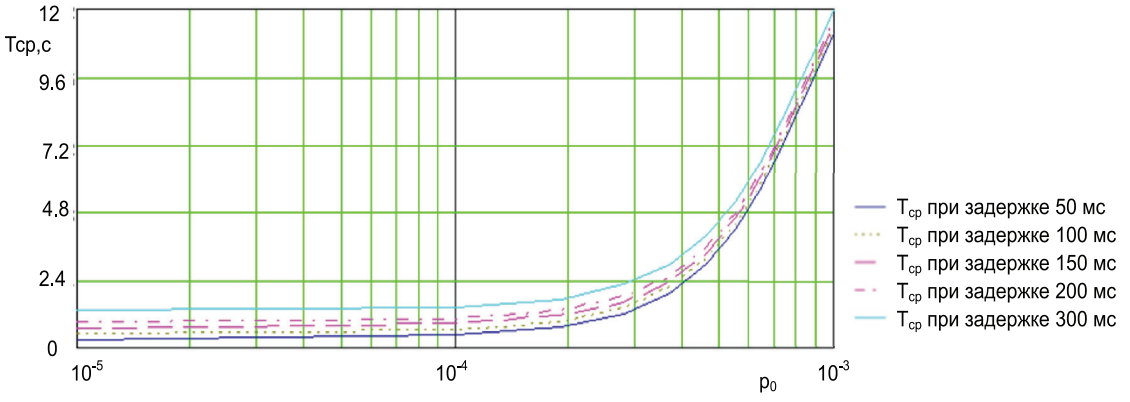


Рис. 5. Зависимость среднего времени выполнения модификации ZRTP

График $T_{CP\_ZZRTP\_MOD}$ для модификации ZRTP приведен на рис. 5. Насколько видно из табл. 2, при $10^{-5} \le p_0 \le 10^{-5}$ и $d = 300$ мс $T_{ZZRTP\_MOD2} \le 1{,}451$ с. Таким образом, поставленная задача о выполнении норм [11] при работе по каналам связи $d \le 300$ мс решена.

Заключение

В статье описаны способы повышения безопасности и улучшения временных характеристик одного из ПРК защищенной IP-телефонии – ZRTP. Исследование показало, что применение способа повышения безопасности ПРК позволяет увеличить безопасность в $1/P_{H1K}$ раз при работе корреспондентов без заранее распределенного ключевого материала за счет использования двух независимых каналов связи, в $1/(P_{H1K})^2$ раз при использовании трех независимых каналов. Для улучшения временных

показателей ПРК предложена модификация протокола, позволяющая успешно выполнять его за то же время, но при работе по каналам с большими значениями задержки и потери пакетов.

Список литературы

1. Агеев С.А., Саенко И.Б. Управление безопасностью защищенных мультисервисных сетей специального назначения // Труды СПИИРАН. – 2010. – № 2(13). – С. 182–198.

2. Бабенко Л.К., Ищукова Е.А. Анализ симметричных криптосистем // Известия Южного федерального университета. Технические науки. – 2012. – № 12 (137). – С. 136–147.

3. Говор Т.А. Обеспечение безопасности современных VOIP-сетей // Радиопромышленность. – 2011. – № 4. – С. 37–43.

4. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. – М.: Стандартинформ, 2013. – 104 с.

5. Докучаев В.А., Шведов А.В. Защита информации на корпоративных сетях VoIP // Электросвязь. – 2012. – № 4. – С. 5–8.

6. Ковцур М.М., Никитин В.Н., Винель А.В. Исследование вероятностно-временных характеристик протокола распределения ключей защищенной IP-телефонии // Информационно–управляющие системы. – 2013. – № 1(62). – С. 54–63.

7. Ковцур М.М., Никитин В.Н., Юркин Д.В. Повышение защиты протоколов распределения ключей от атак вторжения в середину канала связи // Информационно-управляющие системы. – 2014. – № 1(68). – С. 70–75.

8. Ковцур М.М. Протоколы обеспечения безопасности IP-телефонии // Первая миля. – 2012. – № 5. – С. 18–26.

9. Макарова О.С. Методика формирования требований по обеспечению информационной безопасности сети IP-телефонии от угроз среднестатистического «хакера» // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2012. –№ 1 (25), часть 2. – С. 51–67.

10. Нопин С.В. Передача мультимедийных данных по цифровым каналам в режиме, защищенном от несанкционированого доступа: дис. канд. техн. наук. – Новосибирск: Омский государственный технический университет, 2008. – 233 с.

11. Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования [Электронный ресурс]: приказ Министерства информационных технологий и связи Российской Федерации от 27.09.2007 № 113. Минюст РФ 22 октября 2007 г. № 10380. Доступ из справ.-правовой системы «КонсультантПлюс».

12. Perlicki K. Simple analysis of the impact of packet loss and delay on voice transmission quality. // Journal of telecommunications and information technology. – 2002. – № 2. – P. 53–56.

13. RFC6189 (04/2011) – ZRTP: Media Path Key Agreement for Unicast Secure RTP [Электронный ресурс]. – Режим доступа: http://tools.ietf.org/html/rfc6189 (дата обращения: 25.02.2014).

References

1. Ageev S.A., Saenko I.B. Security management of protected multi-service networks for special purposes. *Trudy SPIIRAN*, 2010, vol. 13, no. 2, pp. 182–198.

2. Babenko L.K., Ishhukova E.A. Analysis of simmetric cryptosystems // *Izvestija Juzhnogo federal'nogo universiteta. Tehnicheskie nauki.* 2012, vol. 137, no. 12, pp. 136–147.

3. Govor T.A. Security of modern VOIP-networks. *Radiopromyshlennost'*, 2011 no 4 pp. 37–43.

4. State Standart R ISO/MEK 15408-1-2012. Information technology. security techniques. Evaluation criteria for it security. part 1. Introduction and general model M.: Standartinform, 2013. 104 p.

5. Dokuchaev V.A., Shvedov A.V. Zashhita informacii na korporativnyh setjah VoIP. *Jelektrosvjaz'*, 2012, no. 4, pp. 5–8.

6. Kovtsur M.M., Nikitin V.N., Vinel' A.V. Analysis of the time-probabilistic characteristics of key agreement protocol for secure IP-telephony. *Informacionno–upravljajushhie sistemy,* 2013, vol. 62, no. 1, pp. 54–63.

7. Kovtsur M.M., Nikitin V.N., Jurkin D.V. Enhancement of Security of Key Distribution Protocols against Intruder Attacks in the Middle of a Communication Channel. *Informacionno-upravljajushhie sistemy,* 2014, vol. 68, no. 1, pp. 70–75.

8. Kovtsur M.M. Protocols Providing IP telephony Security. *Pervaja milja,* 2012, no 5, pp. 18–26.

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.

10. Nopin S.V. Peredacha mul'timedijnyh dannyh po cifrovym kanalam v rezhime, zashhishhennom ot nesankcionirovanogo dostupa: dis. kand. tehn. nauk. Novosibirsk: Omskij gosudarstvennyj tehnicheskij universitet, 2008. 233 p.

11. Approval of requirements for organizational and technical support of sustainable operation of PSTN: the order of the Ministry of Information Technologies and Communications of the Russian Federation dated 27.09.2007 № 113. Justice Ministry October 22 2007 № 10380. Available at Legal system «ConsultantPlus».

12. Perlicki, K. Simple analysis of the impact of packet loss and delay on voice transmission quality. *Journal of telecommunications and information technology*, 2002, no 2. pp. 53–56.

13. RFC6189. ZRTP: Media Path Key Agreement for Unicast Secure RTP. 2011. Available at: http://tools.ietf.org/html/rfc6189 (accessed: 25 January 2014).

Рецензенты:

Душин С.Е., д.т.н., профессор кафедры автоматики и процессов управления, СПбГЭТУ «ЛЭТИ», г. Санкт-Петербург;

Комашинский В.И., д.т.н., доцент, советник генерального директора, ЗАО «Институт Телекоммуникаций», г. Санкт-Петербург.

Работа поступила в редакцию 28.07.2014.