УДК 004.056

В.О.Масленников

О ПРОБЛЕМЕ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ КАНАЛОВ ВИДЕОКОНФЕРЕНЦСВЯЗИ

Постановка проблемы. В последнее время, в связи с увеличением пропускной способности каналов связи, становится возможным одновременное общение нескольких абонентов одновременно по каналам аудио и видеосвязи. Такое общение давно известно под названием конференцсвязи, которая раньше реализовывалась исключительно с помощью телефонных каналов связи.

Одновременно с вхождением технологий конференцсвязи в корпоративный сектор, возникает необходимость защиты информации, передаваемой по этим каналам.

Кроме того, с увеличением числа потенциальных пользователей сети, и с внедрением в использование протокола IP ver. 6.0, происходит увеличение децентрализованных одноранговых (P2P — Peer-to-peer) связей между этими пользователями. В рамках сказанного возникает проблема защиты информации, передаваемой при конференцсвязи по открытым каналам связи при одноранговом соединении. В данном случае одноранговое соединение обозначает отсутствие выделенного сервера в сети для хранения информации о пользователях, их открытых ключей, их идентификации.

Основной проблемой при организации безопасной конференцсвязи в одноранговой сети является безопасное распределение ключей шифрования по открытым каналам связи, учитывая отсутствие удостоверяющего центра, который мог бы идентифицировать участников.

Данная проблема в криптографии сводится к протоколу обмена ключами для групп с динамическим составом участников.

В зависимости от модели использования самой конференцсвязи, а, точнее, направления информационных видеопотоков (см. рис.1), целесообразно использование того или иного вида протоколов. Протоколы различаются, в первую очередь, способами обмена информацией между участниками конференцсвязи (см. рис. 2) для генерации единого секретного ключа (ключей), которые впоследствии будут использованы для шифрования видеотрафика потоковым шифром. Причем, каждый из протоколов, должен поддерживать определенный набор операций для одного или нескольких участников, а именно:

1. добавление одного участника в группу;
2. удаление участника из группы;
3. добавление нескольких участников в группу;
4. удаление нескольких участников из группы;
5. другие операции.

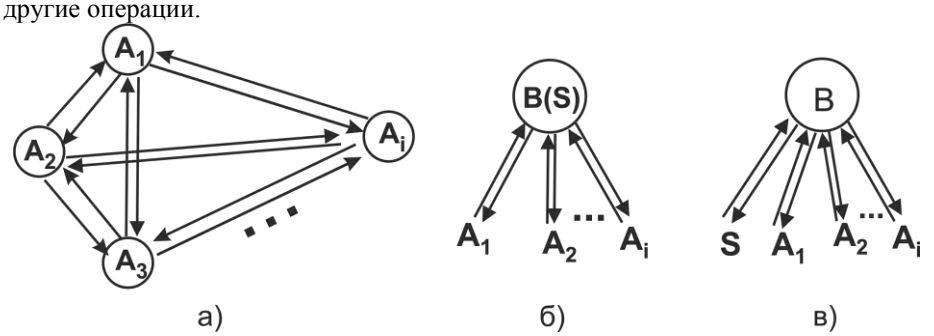

Рис. 1. Информационные потоки при видеоконференцсвязи

В случае, если связь у нас проходит по модели, показанной на рис.1а (достаточно распространённый вариант) — т.е. связь в одноранговой сети между несколькими равноценными участниками, то обмен информацией для реализации протокола создания или обмена секретным ключом (ключами) проходит так, как показано на рис. 2а и 2б. В случае, показанном на рис. 2а для каждой пары абонентов генерируется свой секретный ключ, с помощью которого осуществляется криптографическая защита канала связи. На рис.2б показан более сложный случай группового создания ключа, когда каждый из абонентов «привносит» в ключ свою «часть» секрета. Такой протокол действует по топологии «кольцо» — т.е. информация проходит от первого участника (очевидно, создателя) конференции последовательно к другим, пока последний из участников не выполнит все необходимые вычисления, и не передаст созданный всеми участниками разговора секретный ключ. Такая модель более надежна с точки зрения безопасности и часто используется при большом числе участников. Однако, любая операция с динамической группой участников — добавление, удаление членов, например, требует достаточно большого числа новых вычислений.

Совершенно иная ситуация просматривается, если видеосвязь при конференции идет по принципу, показанному на рис.1б — назовем его условно модель «конференция», или показанному на

рис. 1в — назовем его модель «совещание». При модели «конференция» имеется один узел S (спикер), который транслирует всем участникам свой видеоряд, включая ретрансляцию видеорядов, полученных от других неактивных пользователей. Модель «совещание» отличается тем, что главный узел В (создатель конференции, и периодически выполняющий роль спикера), транслирует видеоряд от текущего выступающего участника (текущего спикера S), а также видеоряды от других неактивных участников (в том числе свой). В обеих этих моделях за прием видеоряда и трансляцию его пользователям отвечает один узел (В). Для криптографической защиты каналов при такой связи достаточно узлу В иметь секретные ключи попарно с каждым абонентом, а каждому абоненту достаточно иметь один секретный ключ для связи с В. Используя соответствующий секретный ключ, В дешифрует нужный видеоряд при приеме, или шифрует при передаче. Шифрование самого видеоряда осуществляется потоковым шифром. Попарную «связку» секретных ключей можно также использовать и в случае, показанном на рис.1а в случае, если количество абонентов достаточно мало (до 10). Кроме того, такой подход применяют в одноранговых сетях для связи двух абонентов по правилу «точка-точка».

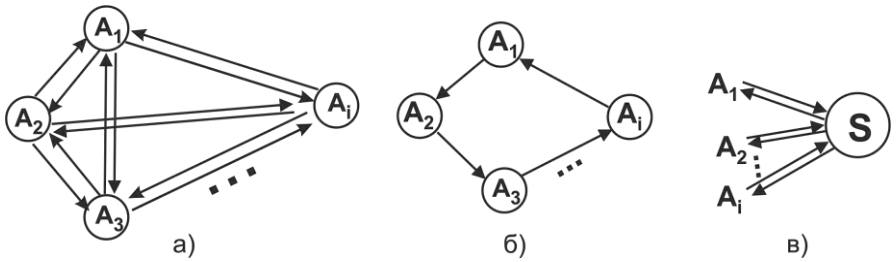

Рис. 2. Обмен информации по криптопротоколу для создания секретного ключа (ключей)

В связи с этим, использование метода попарных «связок» секретных ключей представляется актуальным для защиты каналов видеоконференцсвязи в определенных случаях. Даная статья посвящена описанию применения указанного подхода к случаю с динамической группы из нескольких участников.

Анализ публикаций по теме исследования. Криптографические протоколы, в том числе для систем с динамическим числом участников обсуждается в [1]. Их классификация по предоставляемым сервисам безопасности и используемым математическим методам представлена в [2].

В последнее время в современных криптопротоколах пролеживается тенденция использования математического аппарата эллиптических кривых, который позволяет уменьшить разрядность ключей на десятичный порядок, или, соответственно, увеличить криптостойкость протокола, сохранив разрядность вычислений. Подробно криптопротоколы на эллиптических кривых обсуждаются в [3].

В одноранговых сетях также применяются криптопротоколы, рассмотренные в [2-3], однако модифицированные для защиты от атаки «посредника». Примером такого криптопротокола, реализующего модель, показанную на рисунке 2б, может служить [4]. Проблемы использования криптопротоколов в одноранговых сетях поднимаются также в других публикациях автора статьи.

Цель статьи. В данной статье рассматривается возможность использования криптографического протокола, используемого для защиты передаваемой информации по открытому каналу связи в одноранговой сети между двумя пользователями, для криптографической защиты каналов видеоконференцсвязи между участниками динамической группы из нескольких пользователей. В работе показано, что при некоторых моделях связи использование такого подхода предпочтительней как с точки безопасности, так и с точки зрения объема вычислений.

Основная часть. В одноранговых сетях, при связи двух абонентов, в результате использования криптопротокола, стойкого к атаке «посредника», создается общий секретный ключ шифрования. Этот ключ затем используется потоковым шифром для шифрования/дешифрования передаваемых видеоданных. Примером такого протокола может служить [5].

Покажем, что используя подобные криптопротоколы, можно организовать защиту видеоконференцсвязи в одноранговой сети. Причем, при работе протокола по созданию секретных ключей, информационные потоки будут проходить так, как показано на рисунке 2в.

Криптопротокол разработаем для модели «совещание» (рис. 1в), поскольку модель «конференция» (рис. 1б) является частным случаем модели «совещание». А полносвязную модель (рис. 1а) можно свести к упомянутым моделям при небольшом количестве участников видеоконференции, и приняв абонента, приглашающего остальных к общению, за создателя конференции В. Подробная схема информационных потоков с соответствующими блоками шифрования/дешифрования представлена на рис. 3.

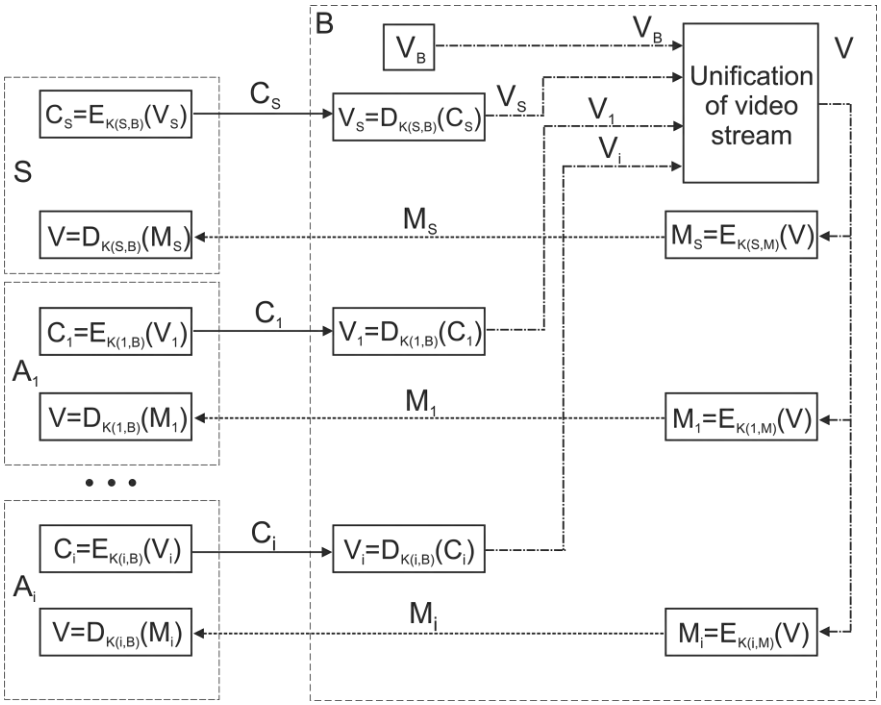

Рис.3. Информационные потоки при видеоконференцсвязи между несколькими участниками в одноранговой сети

В данной модели для шифрования видеотрафика используются секретные ключи, полученные заранее для каждой пары абонентов. Например, абоненты S и B используют общий секретный ключ K(S,B). Каждый абонент i снимает необходимый «свой» видеосигнал V_i, шифрует его при помощи общего с B секретного ключа, используя операцию $C_i = E_{K(i,B)}(V_i)$, и передает по сети пользователю B. Соответственно, абонент B принимает от каждого приглашенного к видеоконференции пользователя зашифрованный сигнал C_i, расшифровывает его с помощью операции $V_i = D_{K(i,B)}(C_i)$. Все полученные сигналы (в т.ч. и V_B) посылаются на специальный модуль «Unification of video stream», задачей которого является «объединение» по определенным правилам полученных сигналов в единый сигнал, которые будет передаваться всем пользователям как текущее состояние всех пользователей конференции. Тут необходимо отметить роль пользователя S (speaker). Это пользователь, который в текущий момент является выступающим, т.е. имеет право говорить. С точки зрения шифрования/дешифрования информационных видеопотоков он ничем не выделяется от остальных, и видеосигнал от этого абонента подлежит такой же обработке. Однако, учитывая возможную функциональность при проведении видеоконференции, может возникнуть необходимость какого-либо особого выделения или обработки этого трафика в модуле «Unification of video stream» — например изображение выступающего должно быть больше изображений неактивных пользователей. Естественно, что возможен частный случай, когда B и S являются одним пользователем, что никаким образом не влияет на модель.

В результате мы видим, что для организации криптографической защиты видеоконференцсвязи в рамках рассмотренной модели, необходимо наличие у каждого пользователя i секретного ключа K(i,B), общего с организатором конференции B.

Обменяться такими ключами или вычислить их позволяют всевозможные криптографические протоколы. При выборе такого протокола следует помнить о возможности выполнения упомянутых выше операций по изменению состава группы участников конференции. Естественно, что имеет смысл для облегчения вычислений выбирать криптопротокол на основе математического аппарата эллиптических кривых, что на порядок уменьшит разрядность участвующих в вычислении значений.

Одним из лучших криптопротоколов для видеоконференцсвязи можно назвать [4]. Однако, в определенных случаях он имеет недостатки. Во-первых, при изменении состава участников — как по одному, так и группой — требуется пересчет секретных ключей. Для небольшого количества пользователей это большая вычислительная нагрузка, учитывая используемый аппарат эллиптических кривых. Во-вторых, поскольку передача информации, согласно архитектуре протокола, идет по топологии «кольцо», все вычисления хранятся у последнего приглашенного абонента. Это не очень хорошо, как с точки зрения криптостойкости, так и с точки зрения управляемости самой видеоконференцией. Т.е. ее создатель не может самостоятельно выбросить или добавить пользователей в конференцию — это должно быть совместным решением. В моделях «совещание» и «конференция» это не всегда удобно.

Рассмотренных недостатков можно избежать, если использовать подход, аналогичный использованному при создании криптопротокола защиты однорангового канала связи между двумя абонентами (см. [5]).

Используя этот подход, необходимо, чтобы абонент B попарно создал секретные ключи с каждым из абонентов i — K(i,B). Криптопротокол для создания такого секретного ключа состоит из четырех шагов.

На первом шаге осуществляется подготовка данных для протокола — генерация случайных значений, участвующих в протоколе и аутентификации, соответствующих параметров эллиптической кривой, а также открытые ключи для передачи другому пользователю.

На втором шаге мы осуществляем двух или более кратную передачу по частям открытых ключей алгоритма шифрования на эллиптической кривой с их хэш-значениями — для защиты от атаки «посредника» (описание соответствующих методов можно найти в [2]).

На третьем шаге, если он присутствует, осуществляется передача аутентифицирующей пользователей информации. Поскольку сеть одноранговая и удостоверяющий центр отсутствует, то под аутентифицирующей информацией понимается некий набор байт, который сам пользователь ввел для своей идентификации (например, строка, описывающая его личные черты, известные только узкому кругу лиц). Возможность обмана со стороны пользователя в данном случае не рассматривается, поскольку в случае одноранговых связей определить его в случае наличия практически невозможно.

Шаг 1. S генерирует:
случайное k_S,
KU_S, KR_S — Открытый и закрытый ключи.
$KU_S=\{KU_S^1||KU_S^2\}$
I_S — аутентифицирующая S информация
B генерирует:
случайное k_B,
KU_B, KR_B — Открытый и закрытый ключи.
$KU_B=\{KU_B^1||KU_B^2\}$
I_B — аутентифицирующая B информация

Шаг 2. Безопасно обмениваемся открытыми ключами:
$S\rightarrow B:\{KU_S^1, H(KU_S,k_S)\}$
$B\rightarrow S:\{KU_B^1, H(KU_B,k_B)\}$
$S\rightarrow B:\{KU_S^2, H(KU_S,k_S)\}$
$B\rightarrow S:\{KU_B^2, H(KU_B,k_B)\}$
$B:KU_S=\{KU_S^1||KU_S^2\}; H(KU_S,k_S)$
$S:KU_B=\{KU_B^1||KU_B^2\}; H(KU_B,k_B)$

Шаг 3. Взаимная аутентификация «двойной» передачей:
$S\rightarrow B: C=E_{KUB}(k_S,I_S)$
$B: D_{KRB}(C)=\{k_S,I_S\}$
B: получает аутентифицирующую S информацию I_S
B: вычисляет $H(KU_S,k_S)$ и убеждается, что KU_S не скомпрометирован
$B\rightarrow S: C=E_{KUS}(k_S,k_B,I_B);$
$S: M=D_{KRS}(C)=\{k_S,k_B,I_B\}$
S: получает аутентифицирующую B информацию I_B, подтвержденную наличием k_S, возвращенным от B (никто другой k_S извлечь бы не смог)
S: вычисляет $H(KU_B,k_B)$ и убеждается, что KU_B не скомпрометирован
$S\rightarrow B: C=E_{KUB}(k_B)$
$B: M=D_{KRB}(C)=\{k_B\}$
B: получив k_B от S, идентифицировал S, т.к. никто другой не мог извлечь k_S.

Шаг 4. Генерация общего секретного ключа:
$S: K=\{k_S||k_B\}$
$B: K=\{k_S||k_B\}$

Рис 4. Криптопротокол генерации общего секретного ключа для создателя видеоконференции B и ее обычного пользователя S.

На четвертом шаге, используя открытые ключи, пользователи в зашифрованном виде передают друг другу сгенерированные на первом шаге случайные значения, из которых создается общий секретный ключ.

Используя описанный подход, протокол создания общего секретного ключа для пользователей S и B может иметь вид как на рис. 4.

Под операциями E и D понимаются соответственно шифрование и дешифрование методом, в основу которого положен математический аппарат эллиптических кривых. Операция H — получение дайджеста сообщения с помощью одной из хэш-функций.

Необходимо заметить, что в качестве идентифицирующей информации может выступать обычная строка, в которой пользователь занес краткие данные о себе личного характера. Если такая взаимная аутентификация не нужна, то шаг 3 можно значительно упростить. В принципе, при необходимости значительно упростить вычисления, можно полностью убрать шаг 3. На общую криптостойкость протокола это не повлияет.

В результате применения данного криптопротокола попарно к пользователям {S,B}, $\{A_1,B\}$, … , $\{A_i,B\}$ у каждого пользователя i появится общий с пользователем B секретный ключ $K(A_i,B)$. С помощью этих секретных ключей и осуществляется шифрование видеосигнала (рис.3).

Одним из особенностей рассмотренного криптопротокола является достаточно легкое добавление и удаление участников. Например, если нам требуется удалить из конференции некоторого участника F, то достаточно, чтобы B из своего множества секретных ключей {K(S,B),K(1,B),…,K(i,B)} удалил K(F,B). Причем, решение об отключении F может принять единолично B. В модели, показанной на рис.3, исчезнет один блок приема видеосигнала и один блок передачи. И никаких иных действий или вычислений не требуется. То же самое касается удаления нескольких участников, добавления одного или нескольких участников. При классическом подходе (например, описанном в [4]), требуется пересчет секретного ключа всеми участниками. Кроме того, в классическом случае требуется либо согласие F на его отключение, либо весь процесс создания конференции с вычислением ключей необходимо повторить заново. В нашем случае таких действий не требуется.

Выводы и перспективы дальнейших исследований. Продемонстрированный подход криптографической защиты видеоконференцсвязи представляется весьма перспективным в некоторых специфических ее видах, а также, при небольшом числе абонентов. Большой интерес в техническом плане представляет возможность использования предложенного криптографического протокола вместе с общепринятыми современными сетевыми сигнальными протоколами, используемыми при конференцсвязи (например, SIP). С программной точки зрения интересно исследовать возможность распределения процессов при шифровании видеопотока от создателя конференции к остальным неактивным участникам.

ЛИТЕРАТУРА:

1. Черемушкин А.В., Криптографические протоколы: основные свойства и уязвимости : учебное пособие для студентов учреждений высшего профессионального образования. / А.В. Черемушкин .—М.:Издательский центр «Академия», 2009.—272 с.
2. Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности: Учебное пособие для вузов / С.В. Запечников.-М.:Горячая линия-Телеком, 2007.-320с.
3. Болотов А.А. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых / А.А. Болотов, С.Б Гашков, А.Б. Фролов. — М.:КомКнига, 2006.—280 с.
4. Фомина И.А. Распределение ключей в группах с динамическим составом участников / И.А. Фомина, А.В. Капренин // Математическое моделирование. Оптимальное управление. Вестник Нижегородского университета им. Н.И.Лобачевского.—2010.—№6.— С.172-177.
5. Масленников В.О. О методе криптографической защиты канала одноранговой связи с использованием протокола Нидхама-Шредера / В.О. Масленников, Н.А. Кондратьева // Вісник Запорізького національного університету. Математичне моделювання і прикладна механіка. — 2009.— №1.—С.123-127.

МАСЛЕННИКОВ Вадим Олегович – старший преподаватель кафедры информационных технологий Запорожского национального университета.

Научные интересы:

- криптология, безопасность сетей, программная архитектура приложений уровня предприятия.