Постановка задачи формирования группового ключа по открытым каналам связи с ошибками

Statement of problem key sharing for group legal users on public noisy channels

Ключевые слова: протокол формирования ключа – key generation protocol; конструктивная модель – structure model; групповой ключ – batch key; канальная связность – connectivity.

Рассматриваемые нами модель канальной связности объектов связи и нарушителя, математическая модель источника, модель нарушителя, протокол формирования группового ключа представляются как процесс формирования группового ключа по открытым каналам связи с ошибками. Предлагается использовать модели случайного кодера и детерминированного декодера для формирования ключа трех объектов связи. Для оценки качества процесса предложены показатели качества и требования к сформированному групповому ключу.

The proposed model to canal coherence legal users and eavesdropper, mathematical model of the source, model of the eavesdropper, key agreement protocol for group legal users introduce as process of the key sharing for group legal users on the of public noisy channels. It is offered use the models casual encoding device and deterministic decoding device for key sharing three legal users. For estimation quality process are offered factors quality and requirements to formed group key.

СИНЮК / SINYUK A.
Александр Демьянович
кандидат технических наук, доцент,
Военная академия связи им. С.М. Буденного,
Санкт-Петербург

Рассмотрим общее описание ситуации передачи информации по каналу. Имеется один передатчик (кодер) у объекта связи (ОС) *A* и три независимо работающих приемника (декодера) у ОС *B*, *C* и нарушителя *E*, на входы которых поступают выходные сигналы разных каналов (рисунок).

На кодер ОС *A* поступают сообщения $\overline{g}$ от источника *G1*, которые он должен передать одновременно приемникам 1, 2 и 3 (объекты связи *B*, *C* и нарушитель *E*) таким образом, чтобы приемники 1 и 2 могли восстановить с произвольно малой вероятностью ошибки сообщения *G1*, а нарушитель не имел этой возможности.

Определение 1. *Модель канальной связности (МКС)* – совокупность, состоящая из источника *G1* и кодера ОС *A*, приемников 1 ОС *B*, 2 ОС *C*, 3 нарушителей *E* и 3 каналов связи между выходом кодера и входами приемников.

Математическое описание представленного выше источника можно дать, используя его статистические характеристики. Пусть источник сообщений *G1* описывается моделью дискретного стационарного источника без памяти [1]. Пусть алфавит источника задается ансамблем $\{G, p(g)\}$, где G – множество, состоящее из t букв $G = \{g_1, ..., g_t\}$. Пусть источник в каждую единицу времени независимо выбирает i-ю букву из алфавита с заданной вероятностью $p(g_i)$ и $\sum_{i=1}^{t} p(g_i) = 1.$

Пусть источник генерирует сообщение $\overline{g}$, представляющее собой последовательность длиной k букв источника, причем $\overline{g} \in G^k$, где G^k – k-я декартова степень множества G. Число последовательностей источника M_0 равно:

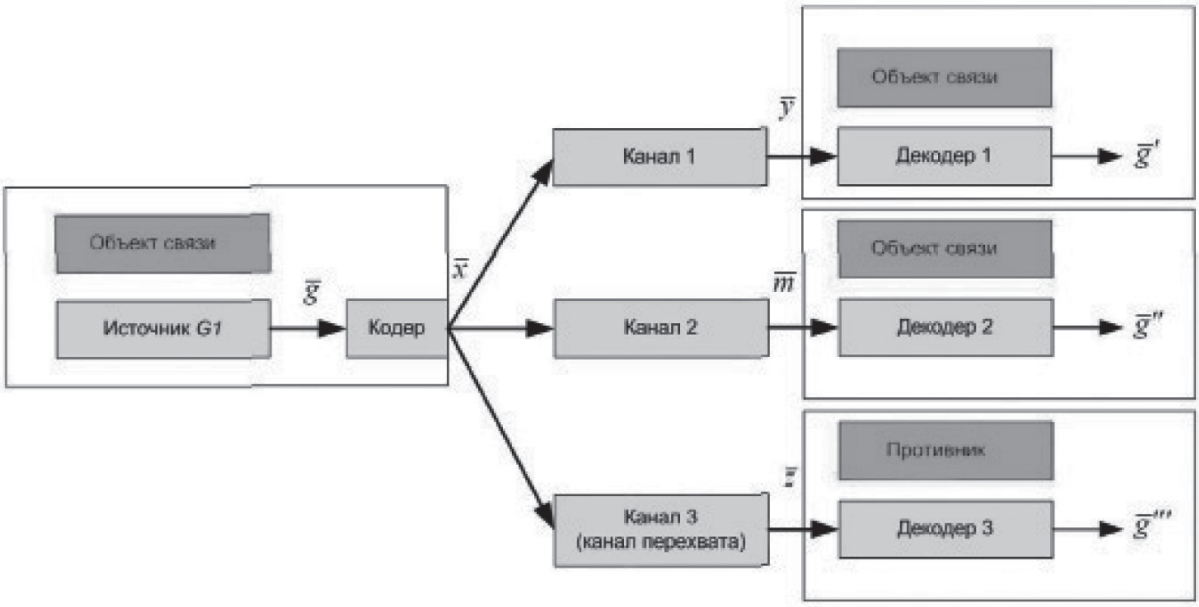
$$\mathrm{M}_0 = t^k. \quad (1)$$

Вероятность последовательности $\overline{g}$ равна:

$$p(\overline{g}) = \prod_{i=1}^{k} p\left(g^{(i)}\right), \quad (2)$$

где $g^{(i)}$ – i-й элемент последовательности $\overline{g}$.

Далее будем полагать, что источник информации стационарен, т.е. вероятности двух одинаковых



Модель канальной связности ОС *A, B, C* и нарушителя *E*

последовательностей, одна из которых занимает временные позиции $g^{(1)},...,g^{(k)}$, другая – временные позиции $g^{(1+j)},...,g^{(k+j)}$, где j – произвольное число, равны:

$$p\left(g^{(1)},...,g^{(k)}\right)=p\left(g^{(1+j)},...,g^{(k+j)}\right)=p\left(\overline{g}\right). \qquad (3)$$

Стационарные случайные последовательности обладают эргодическим свойством [1]. Сделаем предположение, что все каналы связи в МКС описываются моделями дискретных симметричных каналов связи без памяти (ДСК). Совокупность, состоящая из двух каналов с общим входом (выход кодера) и выходами (входы приемников 1, 2), описывается моделью дискретного широковещательного канала без памяти (ДШКБП) [2].

Передача сигналов по ДШКБП определяется двумя *составляющими* каналами ДШКБП с общим входным алфавитом *X,* выходными алфавитами Y и M и матрицами переходных вероятностей $P_1=\{p(y/x)\}, P_2=\{p(m/x)\}, x\in X,\ \ y\in Y, m\in M.$

Алфавиты *X, Y* и M конечны и для любых последовательностей $\overline{x}\in X^n, \overline{y}\in Y^n, \overline{m}\in M^n$, где X^n, Y^n, M^n – декартовые *n*-е степени множеств X, Y, M, соответственно.

$$p\left(\overline{y}/\overline{x}\right)=\prod_{i=1}^{n}p\left(y^{(i)}/x^{(i)}\right), p\left(\overline{m}/\overline{x}\right)=\prod_{i=1}^{n}p\left(m^{(i)}/x^{(i)}\right), \qquad (4)$$

где $x^{(i)}, y^{(i)}, m^{(i)}$ – i-й элемент последовательности $\overline{x}, \overline{y}, \overline{m}$, соответственно.

Определение 2. Канал связи между выходом кодера ОС *A* и входом приемника 3 нарушителя *E* называется *каналом перехвата (КП)*.

Передача сигналов по КП определяется входным конечным алфавитом *X,* выходным алфавитом Z и матрицей переходных вероятностей $P_3=\{p(z/x)\}, x\in X, z\in Z$. Для любых последовательностей $\overline{x}\in X^n, \overline{z}\in Z^n$, где X^n и Z^n – декартовые *n*-е степени множеств *X* и *Z*:

$$p\left(\overline{z}/\overline{x}\right)=\prod_{i=1}^{n}p\left(z^{(i)}/x^{(i)}\right), \qquad (5)$$

где $x^{(i)}, z^{(i)}$ – i-й элемент последовательности $\overline{x}, \overline{z}$, соответственно.

Составляющие ДШКБП и КП являются независимыми каналами:

$$p(y,m\ z/x) = p(y/x) \times p(m/x) \times p(z/x). \qquad (6)$$

Пусть алфавиты источника *G*1, входа и выхода ДШКБП и КП совпадают.

Пусть задано достаточно большое n. Необходимо построить код для передачи информации по ДШКБП. Рассмотрим код, для которого кодер является тождественным отображением на множестве кодовых слов (КС). Код задается множествами КС и декодирующими отображениями, а не кодерами и декодерами [3]. Для передачи информации используем *случайный кодер*. Выберем из множества последовательностей на входе ДШКБП X^n множество КС *V*, причем это множество представляет собой высоковероятное множество типичных последовательностей [4]. Пусть J мощность V не более:

$$J = |V| < 2^{n(F(X;Y;M)-\tau)}, \quad (7)$$

где $F(X;Y;M)$ – средняя совместная информация ДШКБП [2], τ – некоторое положительное число $(\tau > 0)$.

V задает на X^n некоторый (n, ε_1) код со скоростью:

$$R < F(X;Y;M) - \tau. \quad (8)$$

Для (n, ε_1) кода обеспечивается средняя вероятность ошибочного декодирования не более ε_1, $\varepsilon_1 > 0$. Разделим V на M_0 непересекающихся подмножеств $\tilde{N}_i$ равной мощности, где M_0 – общее число последовательностей $G1$ и $i = 1, 2, ..., \mathrm{M}_0$. Тогда D – мощность любого $\tilde{N}_i$:

$$D = \frac{J}{\mathrm{M}_0}. \quad (9)$$

Согласно теореме о высоковероятных множествах [4] для больших n распределение вероятностей на элементах V близко к равномерному и $P(V)$ – вероятность (n, ε_1) кода близка к 1, т.е. для сколь угодно малого ρ, $\rho > 0$:

$$P(V) > 1 - \rho. \quad (10)$$

Тогда распределение вероятностей на элементах $\tilde{N}_i$ близко к равномерному. Кодирование ОС A случайным кодером осуществляется следующим образом. За каждым i-м сообщением $G1$ $\overline{g}_i$ закрепляется соответствующее $\tilde{N}_i$. Если на выходе $G1$ появляется $\overline{g}_i$, тогда кодер выбирает $\tilde{N}_i$. Затем с вероятностью $\frac{1}{D}$ выбирает из последовательностей принадлежащих $\tilde{N}_i$, КС и отправляет его на вход ДШКБП (и КП). Кодирование задает распределение вероятностей на X^n:

$$p(\overline{x}) = \begin{cases} \frac{1}{D} p(\overline{g}_i), & \text{äëÿ âñåõ } \overline{x} \in C_i, \text{ãäå } i = 1, ..., \mathrm{M}_0, \\ 0, & \text{äëÿ âñåõ î ñòàëüíû õ } \overline{x} \notin \bigcup_{i=1}^{\mathrm{M}_0} C_i. \end{cases} \quad (11)$$

Если задан код, тем самым, задано как множество КС, так и правило, по которому приемники принимают решение о переданном КС. Декодирование может осуществляться следующим образом. Объекты связи B и C, зная множества $\tilde{N}_i$, где $1, 2, ..., \mathrm{M}$, выбирают $\tilde{N}_i$ в качестве соответствующих решающих областей $S_i \subseteq Y^n, Q_i \subseteq M^n, i = 1, ..., \mathrm{M}_0$.

Пусть $V1$ – ансамбль решений, который можно рассматривать как результат отображения ансамбля Y^n на выходе первого составляющего канала ДШКБП в множество решающих областей $S_i, ..., S_{\mathrm{M}_0}$. Каждая $\overline{y} \in Y^n$ однозначно определяет решение $v \in V1$ по правилу:

$$v = \begin{cases} v_i, & \text{åñëè } \overline{y} \in S_i, \ i = 1, ..., \mathrm{M}_0, \\ v_{\mathrm{M}_0+1}, & \text{åñëè } \overline{y} \notin \bigcup_{i=1}^{\mathrm{M}_0} S_i. \end{cases} \quad (12)$$

Пусть W – ансамбль решений, который можно рассматривать как отображение ансамбля M^n на выходе второго составляющего канала ДШКБП в множество решающих областей $Q_i, ..., Q_{\mathrm{M}_0}$. Каждая $\overline{m} \in M^n$ определяет решение $w \in W$ по следующему правилу:

$$w = \begin{cases} w_i, & \text{åñëè } \overline{m} \in Q_i, \ i = 1, ..., \mathrm{M}_0, \\ w_{\mathrm{M}_0+1}, & \text{åñëè } \overline{m} \notin \bigcup_{i=1}^{\mathrm{M}_0} Q_i. \end{cases} \quad (13)$$

Для ДШКБП необходимо ввести совместный ансамбль решений. Для каждого кодового слова u_i, $i = 1, ..., \mathrm{M}_0$ определим совместную решающую область L_i, которая объединяет $S_i \subseteq Y^n, Q_i \subseteq M^n$, т.е. $L_i = S_i \cup Q_i$.

Пусть $J1$ — совместный ансамбль решений, который отображает совместный ансамбль $Y^n M^n$ всех пар последовательностей на выходах ДШКБП в множество решающих областей $L_i, ..., L_{\mathrm{M}_0}$. Каждая пара $(\overline{y}, \overline{m}) \in Y^n M^n$ определяет решение $j \in J1$ по следующему правилу:

$$j1 = \begin{cases} j1_i, & \text{åñëè } (\overline{y}, \overline{m}) \in L_i, \ i = 1, ..., \mathrm{M}_0, \\ j1_{\mathrm{M}_0+1}, & \text{åñëè } (\overline{y}, \overline{m}) \notin \bigcup_{i=1}^{\mathrm{M}_0} L_i. \end{cases} \quad (14)$$

Определим вероятность правильного декодирования $Ð_{ïä}$. После передачи КС полная группа событий определяется согласно выражению:

$$\Pr\left((\overline{y}, \overline{m}) \notin \bigcup_{i=1}^{\mathrm{M}_0} L_i \right) + \Pr\left((\overline{y}, \overline{m}) \in \bigcup_{i=1}^{\mathrm{M}_0} L_i \right) = 1, \quad (15)$$

где $\Pr\left((\overline{y}, \overline{m}) \notin \bigcup_{i=1}^{\mathrm{M}_0} L_i \right)$ – вероятность принятия решения j_{M_0+1} согласно (14).

Декодирование осуществляется независимо на выходе каждого составляющего канала ДШКБП

(см. (13) и (12)), и ОС *B* и *C*, зная множества $\tilde{N}_i$, где $i = 1, 2, ..., M_0$ выбрали эти множества $\tilde{N}_i$ в качестве своих соответствующих решающих областей

$S_i \subseteq Y^n, Q_i \subseteq M^n, i = 1, ..., M_0$, тогда согласно (10):

$$\Pr\left(\left(\overline{y}, \overline{m}\right) \notin \bigcup_{i=1}^{M_0} L_i\right) < 1 - (1-\rho)^2. \quad (16)$$

Для вероятности $\Pr\left(\left(\overline{y}, \overline{m}\right) \in \bigcup_{i=1}^{M_0} L_i\right)$ согласно (14) можно записать:

$$\Pr\left(\left(\overline{y}, \overline{m}\right) \in \bigcup_{i=1}^{M_0} L_i\right) = Đ_{ïä} + Đ_{ïä}, \quad (17)$$

где $Đ_{ïä}$, $Đ_{ïä}$ – вероятность правильного и ошибочного декодирования (n, ε_1) кода, соответственно, причем $P_{ïä} < \varepsilon_1$. Тогда искомая $Đ_{ïä}$ равна:

$$P_{ïä} \geq (1-\rho)^2 - \varepsilon_1. \quad (18)$$

Выход КП для нарушителя *E* при использовании случайного кодера представляется случайным выбором сообщения *G*1, что соответствует случайному выбору кодового подмножества, и равномерным распределением входной последовательности на входе КП при условии выбора сообщения *G*1. В этих условиях общая постановка задачи формирования общего ключа (*K*) трех ОС по открытым каналам связи с ошибками сводится к следующему. Необходимо выработать ключ (*K*) для группы из трех ОС, передавая данные по ДШКБП и КП. Требуется обеспечить формирование группового *K* с высокой надежностью для ОС и обеспечить заранее заданный низкий уровень информации об *K* для нарушителя. Нарушитель может только контролировать информацию на выходе КП. После передачи КС ОС обладают некоторой информацией в виде последовательностей на входе ДШКБП и двух его выходах в виде КС $\overline{x}, \overline{x} \in V$ для ОС *A* и принятых $\overline{y}, \overline{y} \in Y^n$ для ОС *B* и $\overline{m}, \overline{m} \in M^n$ для ОС *C*. Они могут быть коррелированы между собой и начальными данными нарушителя в виде $\overline{z}, \overline{z} \in Z^n$. Предполагается, что *E* знает полное описание действий, выполняемых ОС, параметров кода (n, ε_1) и *G*1. Переданная и принятые последовательности не могут быть использованы для формирования *K*, так как в составляющих ДШКБП могут возникать ошибки, и требуют коррекции с использованием метода декодирования. Переданная и декодированные последовательности могут быть выбраны в качестве *K* ОС. В общем виде для большого n протокол формирования *K* представляет следующую последовательность действий:

1. Объект связи *A* с использованием *G*1 генерирует $\overline{g}_i, \overline{g}_i \in G^k$, где $i = 1, ..., M_0$.
2. Объект связи *A* с использованием случайного кодера ставит в соответствие $\overline{g}_i, \overline{g}_i \in G^k$ КС $\overline{x}, \overline{x} \in V$.
3. Объект связи *A* подает $\overline{x}, \overline{x} \in V$ на входы ДШКБП (и КП) и передает его.
4. Объект связи *B* принимает $\overline{y}, \overline{y} \in Y^n$. ОС *C* принимает $\overline{m}, \overline{m} \in M^n$. *E* принимает $\overline{z}, \overline{z} \in Z^n$.
5. Объект связи *B* по правилу декодирования приемника 1 принимает решение о переданном КС. Если $\overline{y} \in S_i$, где $i = 1, ..., M_0$, приемник 1 выносит решение о $\overline{g}_i$ (с вероятностью более, чем $1-\rho$). В результате ОС *B* получает $\overline{g}', \overline{g}' \in G^k$. Если $\overline{y} \notin \cup S_i$ – отказ от декодирования. Объект связи *C* по правилу декодирования приемника 2 принимает решение о КС. Если $\overline{m} \in Q_i$, где $i = i = 1, ..., M_0$, приемник 2 выносит решение о $\overline{g}_i$ (с вероятностью более, чем $1-\rho$). В результате ОС *B* получает $\overline{g}'', \overline{g}'' \in G^k$. Если $\overline{m} \notin \cup Q_i$ – отказ от декодирования.
6. С вероятностью более чем $(1-p)^2$ $\overline{g}', \overline{g}' \in G^k$ выбирается в качестве *K* ОС *B*, $\overline{g}'', \overline{g}'' \in G^k$ выбирается в качестве *K* ОС *C* и $\overline{g}, \overline{g} \in G^k$ выбирается в качестве *K* ОС *A*.

Рассмотрим основные показатели качества переданного *K*. Качественно они сводятся к надежной передаче большого количества бит «хорошего» *K* при малой утечке информации к нарушителю *E*. Выражение (16) показывает, что с вероятностью, отличной от нуля, *K* могут быть не сформированы. Сформированные *K* могут не совпадать, так как они передаются по составляющим ДШКБП с ошибками. Представляет интерес вероятность совокупности этих событий. Обозначим ее P_ε. Очевидно, что P_ε является дополнением к вероятности правильного декодирования $Đ_{ïä}$, определенной в (18):

$$P_\varepsilon = 1 - P_{ïä} < 1 - (1-\rho)^2 + \varepsilon_1. \quad (19)$$

На выходе КП нарушитель *E* получает свою версию переданного КС в виде $\overline{z}, \overline{z} \in Z^n$. Тогда вторым частным показателем качества сформированного ключа целесообразно выбрать *скорость получения информации о K нарушителем E*, которая представляет среднее количество взаимной информации между G^k и Z^n, отнесенное к длине КС *n*, и обозначается I_E:

$$I_E = \frac{1}{n} I\left(G^k; Z^n\right). \quad (20)$$

Важно качество сформированного K в смысле близости распределения ансамбля K к равновероятному распределению вероятностей [5], которое сводится к близости распределения вероятностей букв K к равновероятному распределению вероятностей букв K [1, 3, 4]. Оно определяется параметром Ω, который в общем случае равен [5]:

$$\Omega = \frac{1}{n}\log_2 \mathrm{M}_0 - \frac{1}{n} H\left(G^k\right), \qquad (21)$$

где $H(G^k)$ – энтропия ансамбля выбираемых последовательностей $G1$.

Определим «информационную» скорость формирования K.

Определение 3. Число H_3 называется *скоростью формирования ключа трех ОС*, если для большого n и для сколь угодно малых $\varepsilon_2 > 0$, $\varepsilon_3 > 0$, $\varepsilon_4 > 0$ и $\varepsilon_5 > 0$ при использовании протокола формирования общего K трех О С в рамках предложенной МКС формируется K, который удовлетворяет следующим требованиям:

$$P_\varepsilon < \mathring{a}_2; \qquad (22)$$

$$I_E < \varepsilon_3; \qquad (23)$$

$$\Omega < \varepsilon_4; \qquad (24)$$

$$H_3 < \frac{1}{n} H\left(G^k\right) + \varepsilon_5. \qquad (25)$$

Очевидно, что в требовании (22) $\mathring{a}_2$ с учетом (19) равна:

$$\varepsilon_2 = 1 - (1-\rho)^2 + \varepsilon_1. \qquad (26)$$

Анализ протокола формирования K для трех ОС в рамках МКС с учетом определения H_3 показывает, что он сводится к передаче сообщений по ДШКБП таким образом, чтобы при максимально достижимой H_3 нарушитель не мог восстановить посылаемое сообщение. Для этого необходимо задать рамки изменения скорости кода R, как управляемого ОС A параметра выбираемого (n, ε_1) кода для любого $\varepsilon > 0$ в пределах:

$$\left|\frac{1}{n}\log_2\left(\mathrm{M}_0\right) - R\right| < \varepsilon. \qquad (27)$$

Тогда задача исследования сводится к определению максимально достижимой величины H_3 при максимально возможном R.

Таким образом, в статье произведена постановка задачи формирования группового ключа. Предложена МКС, математическая модель источника, нарушителя (КП, его знания). Предлагается использовать модели случайного кодера и детерминированного декодера (n, ε_1) кода. Для большого n представлен протокол формирования общего K из 6 шагов. Предложены показатели качества сформированного K. Определена «информационная» скорость формирования K, представляющая собой скорость формирования шифрключа для трех ОС H_3. Сформулированы и обоснованы требования к K. Разработанная МКС, выполнение во времени ОС шагов протокола формирования K трех ОС представляется как процесс формирования K трех объектов связи. Задача исследования определяется поиском максимальной H_3 при максимальной скорости кода R.

Литература

1. *Галлагер Р.* Теория информации и надежная связь / Под ред. М.С. Пинскера, Б.С. Цыбакова. – М: Советское радио, 1974.
2. *Синюк А.Д.* Совместная информация трех ансамблей сообщений дискретного широковещательного канала связи без памяти // Информация и космос. – 2010. – № 1. – С. 27–31.
3. *Чисар И., Кернер Я.* Теория информации: теоремы кодирования для дискретных систем без памяти. – М.: Мир, 1985.
4. *Колесник В.Д., Полтырев Г.Ш.* Курс теории информации. – М.: Наука, 1982.
5. *Ahlswede R., Csiszar I.* Common Randomness in Information Theory and Cryptography. – Part I: Secret Sharing // IEEE Trans. on IT. – Vol. 39. – № 4. – July 1993. – P. 1121–1132.