УДК 004.056

О.И. Солонская

Метод обеспечения целостности информации на основе организации параллельных соединений защиты на сетевом уровне

Предложен метод обеспечения целостности информации, основанный на организации параллельных соединений. Представлена оценка вероятности обеспечения целостности, влияние точности измерения вероятности модификации сообщения на принятие решения о переданном символе.

Ключевые слова: информационная безопасность, целостность информации, параллельные соединения, сетевой уровень.

Введение

Решение проблем безопасности инфотелекоммуникационных систем в настоящее время стоит на первом месте, чему способствует всё возрастающее число пользователей и интерактивных информационных ресурсов. В связи с этим возрастает и количество угроз информационной безопасности, в частности, целостности.

Сегодня день базовым подходом обеспечения целостности информации является использование различных криптографических методов и контрольных сумм [2]. При этом в случае модификации информации потребуется повторная передача [3, 4, 6]. Такой подход может значительно снизить качество обслуживания пользователя в случае использования приложений реального времени.

В данной статье рассматривается метод, позволяющий обеспечить целостность информации при помощи организации параллельных соединений. Кроме того, представлен анализ влияния точности измерения отдельных параметров на процесс принятия решения о переданном символе.

Постановка задачи

В [5] представлена суть метода, позволяющего обеспечить целостность информации. Таким образом, при передаче сообщения $S=\{S_1,S_2\}$ с априорными вероятностями появления символов $P(S_1)$ и $P(S_2)$, соответственно, сквозь сеть связи от узла источника к узлу получателя через m транзитных узлов по n параллельным соединениям можно утверждать нижеследующее.

Для решающего устройства (РУ) с n параллельными входами и одновременно принятыми по ним сообщениями $x=(x_1,\ldots,x_i,\ldots,x_n)$ и одним выходом имеет место следующее соотношение:

$$a_0+\sum_{i=1}^{n}x_i a_i=\begin{cases}>0, \text{ то } S^*=S_1,\\ <0, \text{ то } S^*=S_2,\end{cases} \qquad (1)$$

где $a_0=\ln\dfrac{P(S_1)}{P(S_2)}$ и $a_i=\ln\dfrac{\left(1-P_{\text{м}}^{(i)}\right)}{P_{\text{м}}^{(i)}}$ – расчетные коэффициенты; $P_{\text{м}}^{(i)}$ – вероятность модификации символа несанкционированно действующим лицом на соответствующем соединении n ($i=\overline{1,n}$); S^* – восстановленный (принятый) символ.

Тогда оценка вероятности обеспечения целостности информации на выходе РУ в общем виде

$$P_{\text{ц РУ}}=1-\sum_{i=0}^{\frac{n-1}{2}}C_n^{\frac{n+1+2i}{2}}(1-P_{\text{м}})^{\frac{n-1-2i}{2}}P_{\text{м}}^{\frac{n+1+2i}{2}}.$$

Необходимо определить влияние точности измерения параметров, входящих в (1), на функционирование РУ.

Определение точки неустойчивого функционирования РУ

Пусть передается сообщение $S=\{S_1,S_2\}$. На входы РУ поступают символы $x=(x_1,\ldots,x_i,\ldots,x_n)$, после чего восстановленный сигнал S^* отправляется пользователю:

$$S^* = a_0 + \sum_{i=1}^{n} a_i x_i \ .$$

При условии, что $S_1=+1$ и $S_2=-1$, справедливо следующее:

$$S\times S^* = \begin{cases} >0, \text{ нет ошибки на выходе РУ,} \\ <0, \text{ ошибка на выходе РУ.} \end{cases} \qquad (2)$$

Проведем анализ (2), для первого случая. Введем следующие допущения: n = const и нечетное ($i=\overline{3,n}$); $P(S_1)=P(S_2)$; $x_i=S$; $P_{\text{м}}^{(i)}=P_{\text{м}}$.

Тогда

$$S\times S^* = S\left(a_0+\sum_{i=1}^{n}a_i x_i\right) = S\left(\ln 1 + S\sum_{i=1}^{n}\ln\frac{\left(1-P_{\text{м}}\right)}{P_{\text{м}}}\right) = S\times S\times n\times\ln\frac{\left(1-P_{\text{м}}\right)}{P_{\text{м}}} = n\times\ln\frac{\left(1-P_{\text{м}}\right)}{P_{\text{м}}}.$$

В результате, при $P_{\text{м}}=0$, получаем $S\times S^*=\infty$; $P_{\text{м}}=1$, $S\times S^*=-\infty$; $P_{\text{м}}=0{,}5$, $S\times S^*=0$.

В последнем случае наблюдается неустойчивое состояние работы РУ, т.е. неточное вычисление коэффициентов a_i в точке $P_{\text{м}}=0{,}5$ повлечет ошибку на выходе РУ.

Моделирование функционирования разработанного метода, обеспечивающего целостность информации

Организация работы РУ на действующей сети связи повлечет за собой финансовые, организационные и временные затраты. В этой связи целесообразно использовать методы имитационного моделирования. Учитывая, что результаты будут иметь стохастический характер, воспользуемся методом Монте-Карло.

Примем следующие допущения для ожидаемых результатов: точность $\varepsilon=0{,}01$ и достоверность $\alpha=0{,}999$.

Для определения достаточного количества испытаний N при статистическом моделировании воспользуемся выражением из [1]:

$$N = t_\alpha{}^2\,\frac{p(1-p)}{\varepsilon^2}\,, \qquad (3)$$

где t_α – функция, обратная нормальному распределению (при $\alpha=0{,}999$ $t_\alpha=3{,}29$); p – искомая вероятность обеспечения целостности информации.

Из (3) видно, что максимума значение N достигнет при $p=0{,}5$ окончательно получаем:

$$N = 3{,}29^2\,\frac{0{,}5(1-0{,}5)}{0{,}01^2} = 27061\,.$$

При работе алгоритма полагаем $N=30\,000$, в этом случае абсолютная погрешность результатов не ниже 1%.

Основные этапы процесса статистического моделирования (где z – случайное число, генерируемое с помощью датчика случайных чисел по равномерному закону распределения $0\le z\le 1$, $i=\overline{1,N}$, $j=\overline{1,n}$):

– моделирование передаваемого потока сообщений S_i:

$$S = \begin{cases} S_i=+1, \text{ если } z\le P(S_1), \\ S_i=-1, \text{ если } z>P(S_1); \end{cases}$$

– формирование потока x_{ij}, состоящего из N измененных (под действием $P_{\text{м}}$) символов потока S_i, переданных по n параллельным соединениям:

$$x_{ij} = \begin{cases} \text{если } z\le P_{\text{м}}, \text{ то изменение есть, } x_{ij}=S_i\times(-1), \\ \text{если } z>P_{\text{м}}, \text{ то изменения нет, } x_{ij}=S_i; \end{cases}$$

– вычисление коэффициентов a_0 и a_j производится в соответствии с:

$$a_0 = \ln\frac{P(S_1)}{1-P(S_1)}, \qquad a_j = \ln\frac{(1-P_м)}{P_м};$$

– вычисление соотношения (1) для i-го символа переданного по j-соединениям:

$$X_{ij} = a_0 + \sum_{j=1}^{n} x_{ij}a_j;$$

– формирование потока принятых символов S_{ij}^*:

$$S_{ij}^* = \begin{cases} y_{ij} = +1, \text{ если } X_{ij} > 0, \\ y_{ij} = -1, \text{ если } X_{ij} < 0. \end{cases}$$

Программная реализация была выполнена в среде MatLab. Результаты имитационного моделирования представлены на рис. 1.

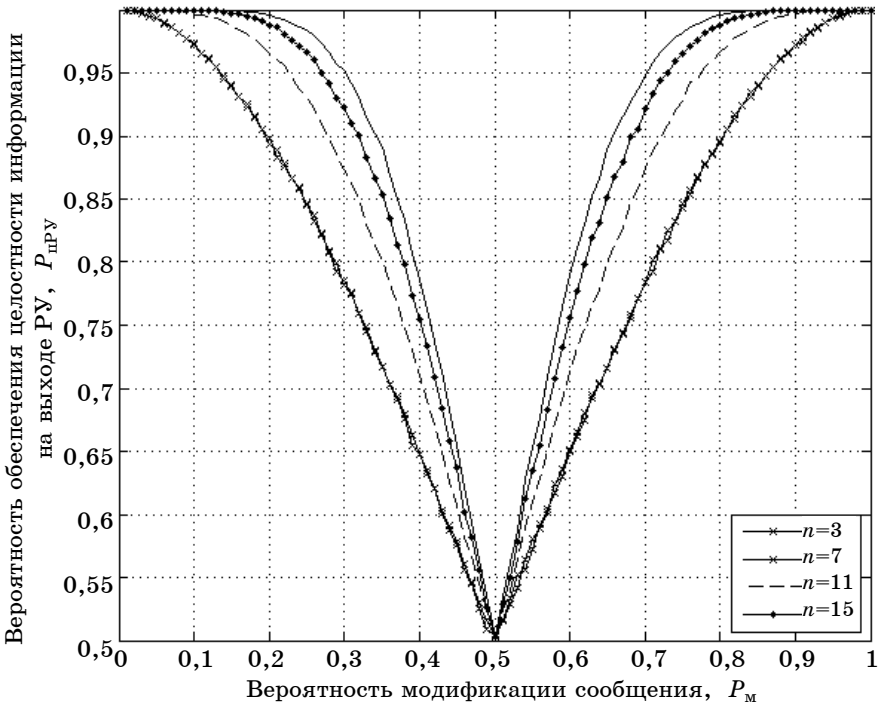

Рис. 1. Семейство графиков зависимости $P_{ц\ РУ} = f(P_м)$ при различном количестве входов РУ

По полученным результатам имитационного моделирования можно сделать следующие выводы: теоретические результаты, совпадают с результатами моделирования; при увеличении вероятности $P_м$ алгоритм позволяет увеличивать вероятность $P_ц$ за счет коэффициентов a_i с точкой перегиба в $P_м = P_ц = 0{,}5$.

Анализ влияния точности измерения $P_м$ на результат работы РУ

Так как в выражение для вычисления a_i входит вероятность модификации сообщения $P_м$, которая имеет случайный характер, то можно предположить, что точность ее определения будет влиять на результаты моделирования в целом. В этой связи проведем с помощью статистического моделирования анализ влияния точности $P_м$ на принятие решения о передаваемой сообщении. Результаты моделирования представлены на рис. 2–4 при $n = 7$.

Анализ полученных результатов моделирования позволяет сделать вывод, что значения вероятности целостности $P_{ц\ ру}$, полученные при $P_м$ и ($P_м \pm \Delta$) и малых погрешностях (менее 5%), не изменяются во всем диапазоне, кроме областей, близких к «0,5» ($0{,}45 < P_м < 0{,}55$) и к «1» ($0{,}95 < P_м < 1$). Это обусловлено тем, что сохраняются взаимные влияния между коэффициентами a_i.

Итоговая зависимость $P_{ц\ РУ} = f(P_м, \Delta)$ результатов моделирования приведена в таблице.

По полученным результатам имитационного моделирования можно сделать следующие выводы:

– при незначительном изменении величины $P_м$ на ($P_м \pm \Delta$) значение $P_{ц\ РУ}$ не изменяется, так как сохраняются взаимные отношения коэффициентов a_i;

– значение $P_{ц\ РУ}$ резко падает при прохождении определенного порога погрешности Δ, что показано в таблице.

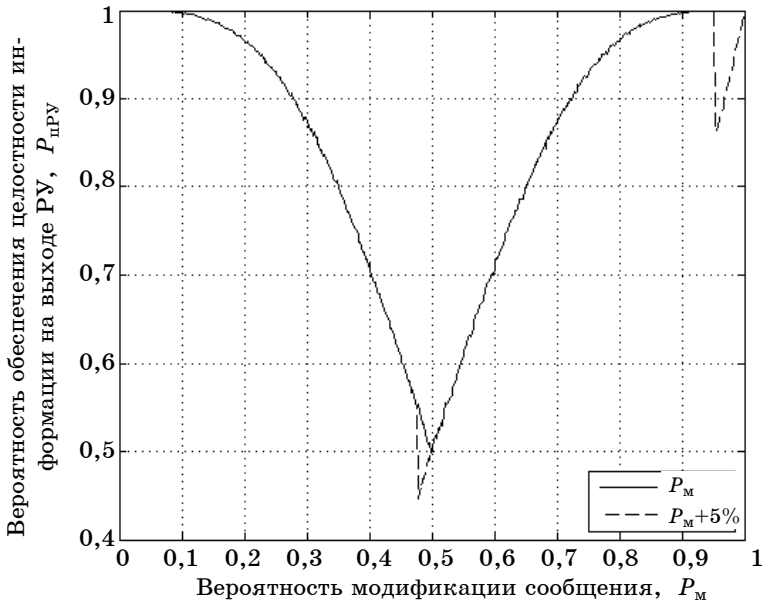

Рис. 2. Графики зависимостей $P_{цРУ} = f(P_м)$ и $P_{цРУ} = f(P_м + 5\%)$

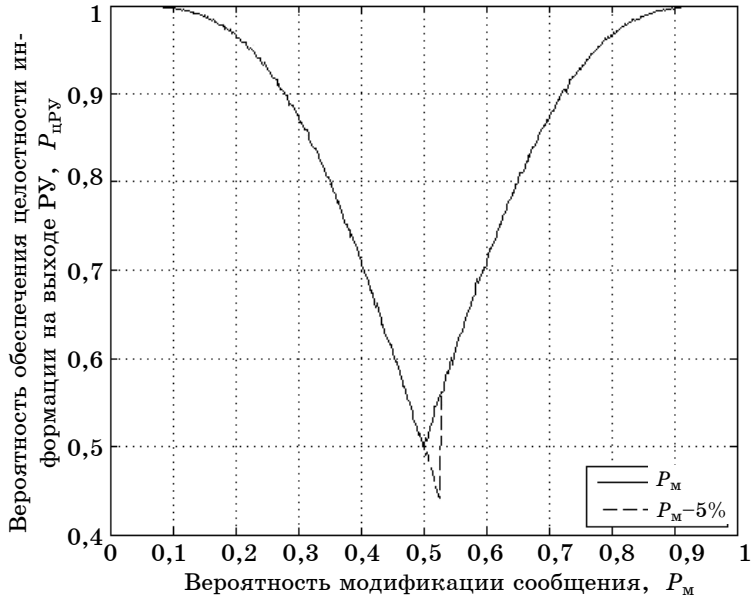

Рис. 3. Графики зависимостей $P_{цРУ} = f(P_м)$ и $P_{цРУ} = f(P_м - 5\%)$

Сводная таблица допустимых погрешностей для $P_м$

$P_м$	Диапазон допустимых погрешностей Δ, %	$P_м$	Диапазон допустимых погрешностей Δ, %
0,1	$-100 < \Delta \le 100$	0,6	$-16{,}67 < \Delta < 66{,}67$
0,2	$-100 < \Delta \le 100$	0,65	$-23{,}09 < \Delta < 53{,}85$
0,25	$-100 < \Delta < 100$	0,7	$-28{,}58 < \Delta < 42{,}86$
0,3	$-100 < \Delta < 66{,}70$	0,75	$-33{,}34 < \Delta < 33{,}33$
0,35	$-100 < \Delta < 42{,}90$	0,8	$-37{,}50 < \Delta < 25{,}00$
0,4	$-100 < \Delta < 25{,}00$	0,85	$-41{,}18 < \Delta < 17{,}65$
0,45	$-100 < \Delta < 11{,}12$	0,9	$-44{,}45 < \Delta < 11{,}11$
0,5	$\Delta = 0$	0,95	$-47{,}37 < \Delta < 5{,}26$
0,55	$-9{,}10 < \Delta < 81{,}82$	1	$-50 < \Delta < 0$

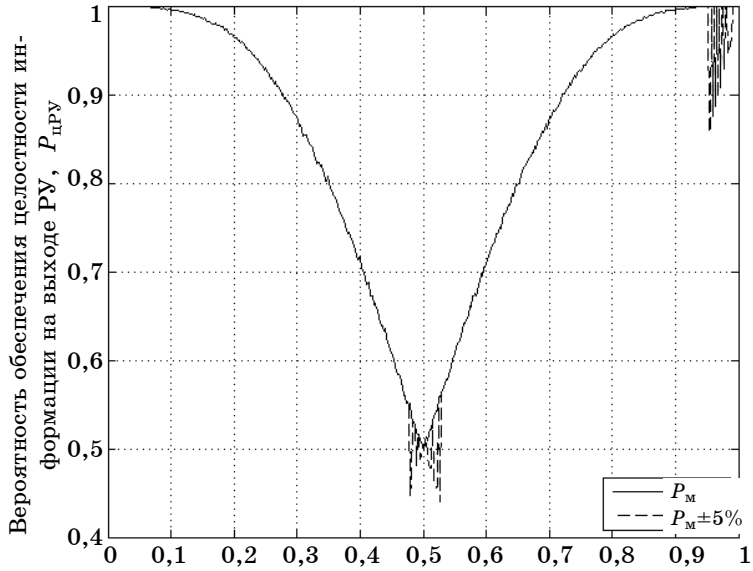

Рис. 4. Графики зависимостей $P_{цРУ} = f(P_м)$ и $P_{цРУ} = f(P_м \pm 5\%)$

Выводы

1. Предложенный метод позволяет обеспечивать требуемый уровень целостности пользовательской информации даже при больших значениях вероятности модификации сообщений.

2. Точка $P_м = 0{,}5$ является точкой неустойчивой работы РУ.

3. Из результатов моделирования также видно, что точность измерения коэффициентов a_i существенно влияет на работу РУ. Необходимо формировать базу данных статистических данных об изменении вероятности модификации сообщений. График на рис. 3 выполнен с учетом полных знаний о $P_м$.

Литература

1. Бусленко Н.П. Моделирование сложных систем. – М.: Наука, 1968. – 356 с.

2. Домарев В.В. Защита информации и безопасность компьютерных систем. – К.: ДиаСофт, 1999. – 480 с.

3. Кларк Дж. мл. Кодирование с исправлением ошибок в системах цифровой связи: пер. с англ. / Дж. Кларк мл., Дж. Кейн. – М.: Радио и связь, 1987. – 392 с.

4. Мелентьев О.Г. Теоретические аспекты передачи данных по каналам с группирующимися ошибками / Под ред. профессора В.П. Шувалова. – М.: Горячая линия–Телеком, 2007. – 232 с.

5. Новиков С.Н. Обеспечение целостности в мультисервисных сетях / С.Н. Новиков, О.И. Солонская // Докл. Том. гос. ун-та систем управления и радиоэлектроники. № 1 (19), ч. 2. – 2009. – С. 83–85.

6. Шувалов В.П. Прием сигналов с оценкой их качества. – М.: Связь, 1979. – 237 с.

Солонская Оксана Игоревна
Ст. преп. каф. безопасности и управления в телекоммуникациях (БиУТ)
Сибирского государственного университета телекоммуникаций и информатики, г. Новосибирск
Тел./факс: (+7-383-2) 69-82-45, моб. тел. +7-913-938-36-85
Эл. адрес: solonskaya@gmail.com

O.I. Solonskaya

Method of user information securing integrity based on parallel link organization at the open system interconnection network layer

Information integrity method is offer, which base on parallel link organization.
Information integrity probability is estimate, influence of message modification probability measurement accuracy on decision making about transmitted symbol.
Keywords: information security, integrity of information, parallel links, network layer.