УДК 004.056 ББК 32.973.2

С.Н. Новиков, О.И. Солонская

Обеспечение целостности в мультисервисных сетях

Предложен алгоритм обеспечения целостности передаваемой информации на сетевом уровне модели взаимодействия открытых систем. Получена формула, дающая возможность количественной оценки целостности сообщения.
Ключевые слова: целостность, компьютерная сеть, сообщение, защита информации.

Обеспечение информационной безопасности является обязательным требованием к современным сетям связи, которая сводится к организации функционирования соответствующих сервисных служб [1]. Основными методами реализации целостности передаваемой информации (ЦПИ) являются: внесение избыточности в передаваемый сигнал [2]; использование обратной связи [3], что ограничивает их применение для приложений, функционирующих на высоких скоростях и критичных к задержкам (например, видеоконференции). В статье предлагается вариант реализации ЦПИ, состоящий в том, что на сети между источником и получателем информации, с помощью сетевых протоколов, организуется n параллельных соединений. В данном случае обеспечение ЦПИ сводится к процедуре принятия решения решающим устройством (РУ) в точке приема по n одновременно принятым сообщениям [4].

I. Синтез РУ, обеспечивающего целостность передаваемой информации

Предположим, что источник информации генерирует сообщения $S=\{S_i\}$; $i=1, 2$ с априорными вероятностями их появления в каждом из n параллельных соединениях

$$0 \le P(S_i) \le 1; \quad \sum_{i=1}^{n} P(S_i) = 1.$$

В каждом из n соединений допускается модификация передаваемых сообщений S в $X=(x_1,\ldots,x_j,\ldots,x_n)$ с независимыми вероятностями $P_{\text{м}}^{(j)}$; $j=\overline{1,n}$.

Тогда для РУ с n параллельными входами $\{x_j\}$, $j=\overline{1,n}$ и одним выходом Y имеют место следующие соотношения:

$$\frac{P\left\{S_1/\left(x_j; i=\overline{1,n}\right)\right\}}{P\left\{S_2/\left(x_j; i=\overline{1,n}\right)\right\}} = \frac{P(S_1)}{P(S_2)} \times \frac{\prod\limits_{i\in x_j=S_1}\left(1-P_{\text{м}}^{(j)}\right)}{\prod\limits_{j\in x_j=S_1} P_{\text{м}}^{(j)}} \times \frac{\prod\limits_{i\in x_j=S_2} P_{\text{м}}^{(j)}}{\prod\limits_{j\in x_j=S_2}\left(1-P_{\text{м}}^{(j)}\right)};$$

$$\ln\frac{P\left\{S_1/\left(x_j; j=\overline{0,n}\right)\right\}}{P\left\{S_2/\left(x_j; j=\overline{0,n}\right)\right\}} = \ln\frac{P(S_1)}{P(S_2)} + \sum_{j\in x_j=S_1}\ln\frac{\left(1-P_{\text{м}}^{(j)}\right)}{P_{\text{м}}^{(j)}} + \sum_{j\in x_j=S_2}\frac{P_{\text{м}}^{(j)}}{\left(1-P_{\text{м}}^{(j)}\right)},$$

где

$$P\left\{S_1/\left(x_j; j=\overline{1,n}\right)\right\}, \quad P\left\{S_2/\left(x_j; j=\overline{1,n}\right)\right\},$$

соответственно, условные вероятности, того, что на выходе РУ будет сигнал S_1 или S_2.

Допустим, что $S_1=+1$; $S_2=-1$, тогда:

$$\ln\frac{P\left\{S_1/\left(x_j; i=\overline{0,n}\right)\right\}}{P\left\{S_2/\left(x_j; i=\overline{0,n}\right)\right\}} = a_0 + \sum_{j=1} x_j a_j,$$

где

$$a_0 = \ln\frac{P(S_1)}{P(S_2)}; \quad a_j = \ln\frac{\left(1-P_{\text{м}}^{(j)}\right)}{P_{\text{м}}^{(j)}}$$

Таким образом, алгоритм принятия решения для обеспечения целостности переданной информации следующий:

$$a_0 + \sum_{j=1}^{n} x_j a_j \begin{cases} > 0, & \text{то} \quad Y = S_1, \\ < 0, & \text{то} \quad Y = S_2. \end{cases}$$

Функциональная схема РУ представлена на рис. 1.

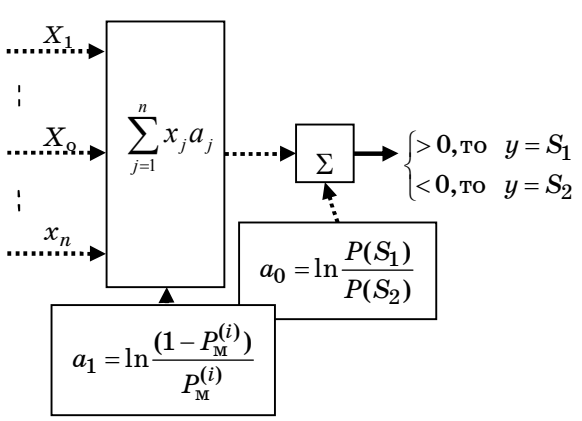

Рис. 1. Функциональная схема РУ

II. Оценка вероятности целостности принятой информации

Пусть вероятности модификации по n входам РУ независимы и равны между собой:

$$P_м = P_м^{(j)}; \quad j = \overline{1,n}.$$

Тогда вероятность ошибочного решения на выходе РУ (при условии, что n нечетно)

$$P_{О\,РУ} = \sum_{i=0}^{\frac{n-1}{2}} C_n^{\frac{n+1+2i}{2}} (1 - P_м)^{\frac{n-1-2i}{2}} P_м^{\frac{n+1+2i}{2}}.$$

Соответственно, вероятность целостности принятой информации будет

$$P_ц = 1 - \sum_{i=0}^{\frac{n-1}{2}} C_n^{\frac{n+1+2i}{2}} (1 - P_м)^{\frac{n-1-2i}{2}} P_м^{\frac{n+1+2i}{2}}.$$

На рис. 2 приведены графики зависимостей $P_ц = f(n)$ при различных $P_м$.

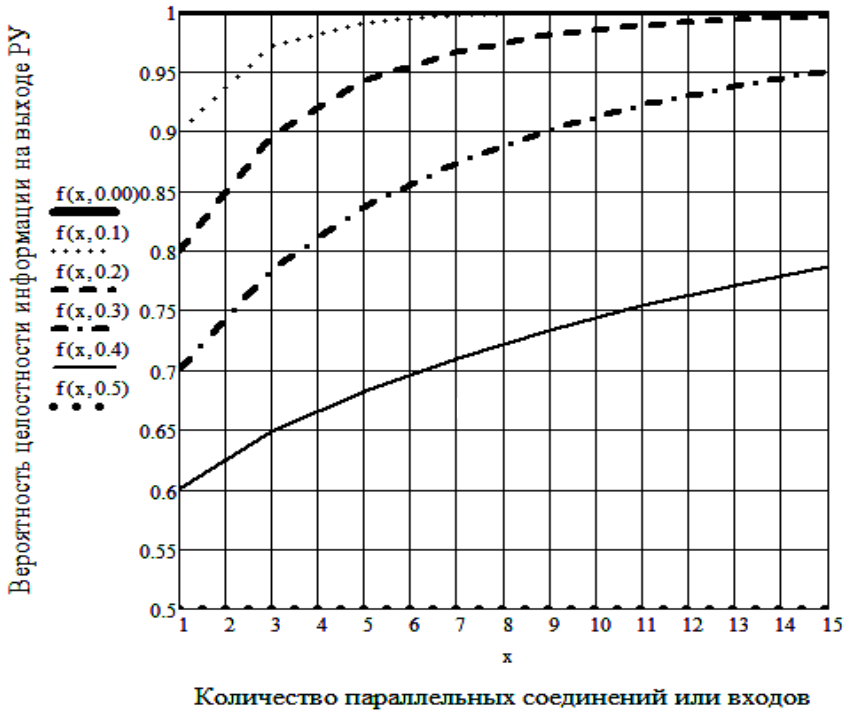

Рис. 2. График зависимостей $P_ц = f(n)$ при различных $P_м$

Выводы

1. Разработан алгоритм, обеспечивающий целостность передаваемой информации на сетевом уровне.

2. Получена формула, дающая возможность количественной оценки целостности передаваемой информации по сети связи.

Литература

1. ATM Security Specification Version 1.1 – March, 2001.

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

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

4. Новиков С.Н.Обеспечение информационной безопасности на сетевом уровне модели взаимодействия открытых систем в мультисервисных сетях / С.Н. Новиков, О.И. Солонская // Матер. X Междунар. конф. «Проблемы функционирования информационных сетей». – Новосибирск. 2008. – С. 81–86.

Новиков Сергей Николаевич
ГОУ ВПО «Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ),каф. «Безопасность и управление в телекоммуникациях» (БиУТ),
к.т.н., доцент, зав. каф. БиУТ,
Эл. адрес: snovikov@ngs.ru, snovikov@mbit.ru

Солонская Оксана Игоревна
ГОУ ВПО «Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ),каф. «Безопасность и управление в телекоммуникациях» (БиУТ),
ст. преподаватель каф. БиУТ
Эл. адрес: solonskaya@gmail.com

S.N. Novikov,O.I. Solonskaya

Securing integrity in multiservice networks

Algorithm of transmitted information securing integrity at the open system interconnection network layer is suggested. A formulation to enable a quantitative assessment of the information integrity is made.

Keywords: integrity, a computer network, the message, information security.
