УДК 004.896:004.451.25

Ю.В. Мельник

ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЇ НА МЕРЕЖЕВОМУ РІВНІ МУЛЬТИСЕРВІСНИХ МЕРЕЖ ЗВ'ЯЗКУ

Розроблений метод забезпечення цілісності і доступності інформації на базі технологій мережевого рівня мультисервісних мереж зв'язку. Розглянута структурна схема вирішувального пристрою. Запропоноване правило прийняття рішення щодо оцінки цілісності інформації. Наведені результати імітаційного моделювання роботи вирішувального пристрою.

Ключові слова: ймовірність модифікації, доступність інформації, ймовірність цілісності інформації.

Вступ

Одним з шляхів забезпечення комплексного захисту інформації без зниження QoS є використання ресурсів мультисервісної мережі зв'язку (ММЗ). Користувачу, при цьому, достатньо визначитись з профілем захисту, а саме з кількісними оцінками конфіденційності, цілісності та доступності інформації. Система керування, за результатами моніторингу вільних ресурсів ММЗ, реалізує не тільки з'єднання яке підтримує QoS для даного додатку, але і заявлений користувачем профіль вимог. Реалізація даного підходу цілком можлива за рахунок протоколів маршрутизації і сигналізації.

Основна частина

Реалізація паралельної передачі та обробки інформації в точці прийому є одним з ефективних методів, що забезпечують надійність обчислювальних і телекомунікаційних систем [1-3]. Застосуємо даний підхід для забезпечення цілісності інформації з підтриманням показників QoS високошвидкісних додатків мереж зв'язку, що функціонують в реальному масштабі часу.

Нехай в мережі між вузлом джерелом (ВД) і вузлом отримувачем (ВО) передається повідомлення, що представляє собою потік бітів $M = \{M_1, M_2\}$ з відповідними апріорними ймовірностями $P(M_1)$ і $P(M_2)$.

Повідомлення передається від ВД до ВО по n паралельним з'єднанням через m транзитних вузлів (ТВ) в кожному з'єднанні (Рис. 1).

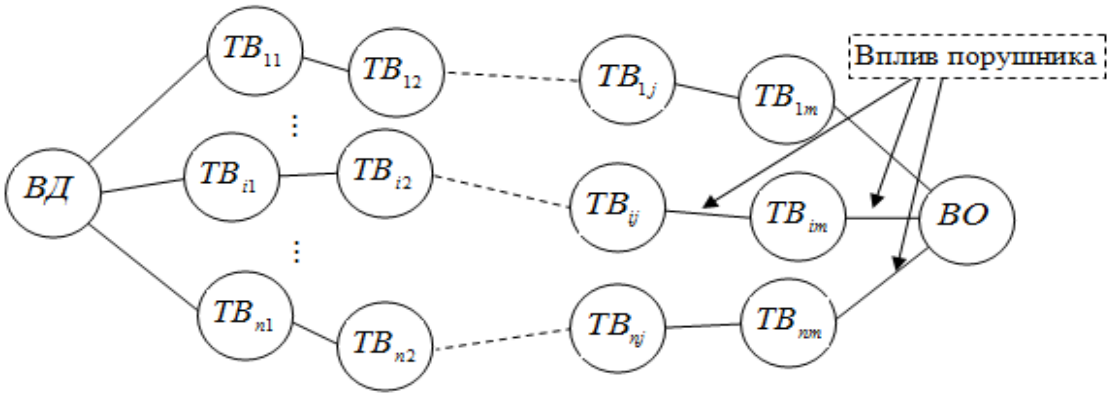

Рис. 1 Організація паралельних з'єднань

Нехай $P_M^{(i)}$ - ймовірність модифікації повідомлення внаслідок атаки порушника в відповідному i - му з'єднанні $\left(i = \overline{1,n}\right)$.) В даному випадку цілісність інформації досягається за рахунок прийняття рішення в ВО по n прийнятим символам. В результаті, значення $M*$ на виході вирішувального пристрою (ВП) буде відповідати переданому значенням M_1 або M_2.

Умовні ймовірності прийняття рішення на користь M_1 або M_2, відповідно, визначаються як [4]

$$P\left(M_1/\left(x_i;i=\overline{1,n}\right)\right)=\frac{P\left(M_1\right)\left\{\prod_{i;x_i=M_1}\left(1-P_M^{(i)}\right)\cdot\prod_{i;x_i=M_2}P_M^{(i)}\right\}}{P\left(x_i;i=\overline{1,n}\right)}$$

$$P\left(M_2/\left(x_i;i=\overline{1,n}\right)\right)=\frac{P\left(M_2\right)\left\{\prod_{i;x_i=M_2}\left(1-P_M^{(i)}\right)\cdot\prod_{i;x_i=M_1}P_M^{(i)}\right\}}{P\left(x_i;i=\overline{1,n}\right)}$$

Візьмемо відношення цих виразів. Якщо результат виявиться більше 1, то приймаємо рішення на користь M_1, в іншому випадку M_2. Після логарифмування відношення і деяких перетворень отримаємо вираз

$$\ln\frac{P\left\{M_1/\left(x_i;i=\overline{1,n}\right)\right\}}{P\left\{M_2/\left(x_i;i=\overline{1,n}\right)\right\}}=a_0+\sum_{i=1}^{n}x_i\cdot a_i \qquad (1)$$

де $a_0=\ln\frac{P\left(M_1\right)}{P\left(M_2\right)};\ a_i=\ln\frac{1-P_M^{(i)}}{P_M^{(i)}}$

Таким чином, має місце наступне правило прийняття рішення [2]:

$$a_0+\sum_{i=1}^{n}x_i\cdot a_i\begin{cases}якщо>0\Rightarrow M^*=M_1\\якщо<0\Rightarrow M^*=M_2\end{cases} \qquad (2)$$

Функціональна схема ВП приведена на рис. 2.

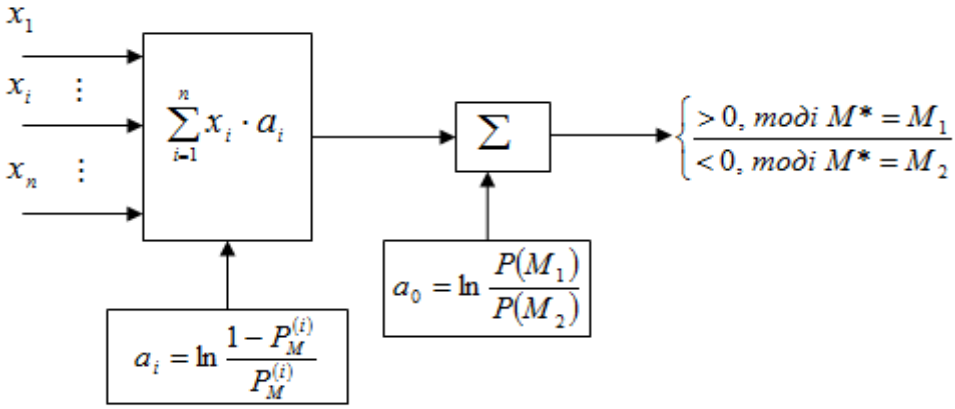

Рис. 2. Функціональна схема вирішувального пристрою

Оцінимо ймовірність цілісності інформації в мережі.

Введемо наступні обмеження:

- ймовірності модифікації $M=\{M_1,M_2\}$ по всіх з'єднаннях між ВД і ВО рівні, тобто $P_M=P_M^{(i)};\ i=\overline{1,n}$ і незалежні (рисунок 1);
- кількість паралельних з'єднань n між ВД і ВО непарні і $n\geq 3$.

Тоді ймовірність цілісності інформації (рисунок 2.) визначається виразом [2]:

$$P_{Ц\,ВП} = 1 - \sum_{i=0}^{(m-1).2} C_n^{(n+1+2\cdot i)/2} \cdot \left(1 - P_M\right)^{\left(n-1-2\cdot i\right)/2} \cdot P_M^{(n+1+2\cdot i)/2} \qquad (3)$$

де - $C_n^{(n+1+2\cdot i)/2}$ число поєднань $(n+1+2\cdot i)/2$ з n.

На Рис. 3. наведені результати оцінки цілісності інформації, розраховані за формулою (3).

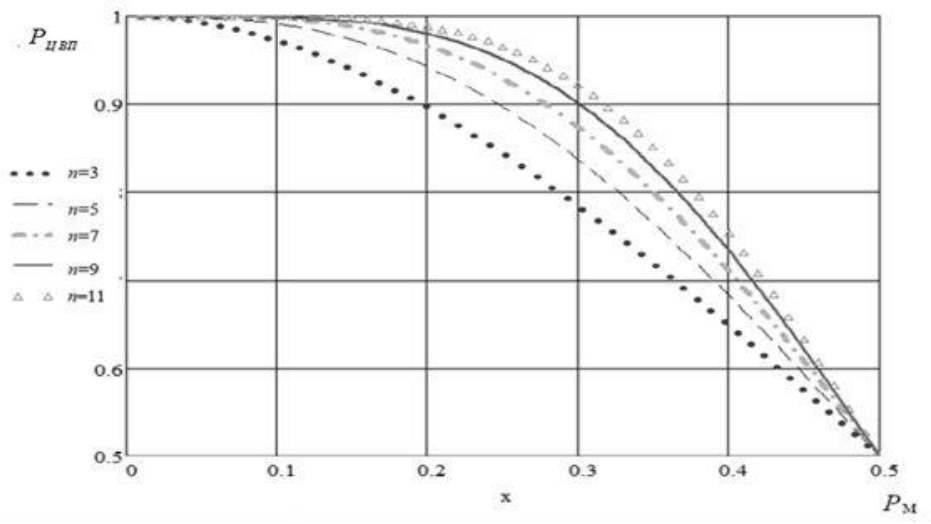

Рис. 3. Результати теоретичного розрахунку $P_{Ц\,ВП} = f(P)$ для різних значень n.

Для уникнення фінансових та організаційних труднощів при перевірці функціонування ВП (Рис. 2), що реалізує алгоритм (2), на діючій мережі зв'язку при підтвердженні теоретичних результатів оцінки ймовірності цілісності інформації на виході ВП доцільно скористатися методом статистичного моделювання [4].

Вихідними даними алгоритму моделювання є:

- $P(M_1)$ і $P(M_2)$ - апріорні ймовірності появи $M = \{M_1, M_2\}$ на виході ВД при умові $P(M_1) + P(M_2) = 1$;

n - кількість з'єднань між ВД і ВО;

$P_M = P_M^{(i)}; i = \overline{1,n}$ - ймовірності модифікації бітового потоку $M = \{M_1, M_2\}$ на виході ВД з n з'єднаннями між ВД і ВО;

N_0 - кількість переданих значень $M = \{M_1, M_2\}$ між ВД і ВО (кількість незалежних випробувань при статистичному моделюванні).

Здійснюємо N_0 випробувань кожне з яких складається з чотирьох етапів. На першому етапі формується випадковий бітовий потік $M = \{M_1, M_2\}$ за правилом:

$$M = \begin{cases} +1 \text{ якщо } z_k \le P(M_1) \\ -1 \text{ якщо } z_k > P(M_1) \end{cases}$$

де z_k - випадкове число яке генерує датчик випадкових чисел з рівномірним законом розподілу $0 \le z_k \le 1; k = \overline{1, N_0}$

На другому етапі модифікуються значення $M=\{M_1,M_2\}$ в кожному з n встановлених паралельних з'єднаннях між ВД і ВО:

$$x_i=\begin{cases}\text{якщо } z_k \le P_M, \text{ то модіфікація є, } x_i=M\times(-1)\\ \text{якщо } z_k > P_M, \text{ то модіфікації нема, } x_i=M\end{cases}$$

На третьому етапі розраховуються коефіцієнти $a_0=\ln\frac{P(M_1)}{P(M_2)}; a_i=\ln\frac{1-P_M^{(i)}}{P_M^{(i)}}$ і приймається рішення за правилом (2).

На четвертому етапі перевіряється правильність прийняття рішення за правилом (2) і підрахунок $N+$ - кількості правильно прийнятих значень $M=\{M_1,M_2\}$ з N_0 переданих.

На п'ятому етапі визначається оцінка ймовірності цілісності інформації на виході вирішувального пристрою:

$$P_{Ц\,ВП}=\frac{N+}{N_0}$$

Метод статистичного моделювання є наближеним. Похибка результату обчислення має статистичну природу. Кількісний взаємозв'язок між абсолютною похибкою і числом випробувань N_0 визначається як [5]:

$$\Delta_a=N_0^{-0,5}\cdot\sigma\cdot t_\beta \tag{4}$$

де Δ_a - абсолютне значення похибки (половина довірчого інтервалу; σ - середньоквадратичне відхилення від $P_{Ц\,ВП}$; β - достовірність оцінки що отримується; t_β - таблична функція зворотна нормальній при аргументі $(1+\beta)^{-1}$.

Визначимо скільки необхідно провести випробувань, щоб забезпечити задану абсолютну або відносну похибку обчислення. З (4) легко отримати шукану величину:

$$N_0=t_\beta^2\cdot\sigma^2\cdot\Delta_a^{-2} \tag{5}$$

Результати оцінки цілісності інформації на виході ВП (Рис. 2.) методом статистичного моделювання (програмна реалізація виконана в середовищі MatLab) представлені на Рис. 4.

Результати імітаційного моделювання підтверджують теоретичні розрахунки за формулою (3).

Резервування каналів зв'язку і дублювання самої інформації є базовими методами забезпечення доступності інформації ТКМ [1, 2]. Це, як правило, реалізується за рахунок організації паралельних з'єднань між ВД і ВО (Рис. 1). Нехай c_i - вартість i- го з'єднання між ВД і ВО. Тоді загальна вартість організації n паралельних з'єднань буде $c_0=\sum_{i=1}^{n}c_i$.

Якщо вважати вплив порушників на кожне з'єднання незалежними подіями, то результуючу ймовірність забезпечення цілісності інформації можна визначити як

$$P_{рез}=1-\prod_{i=1}^{n}(1-p_i) \tag{6}$$

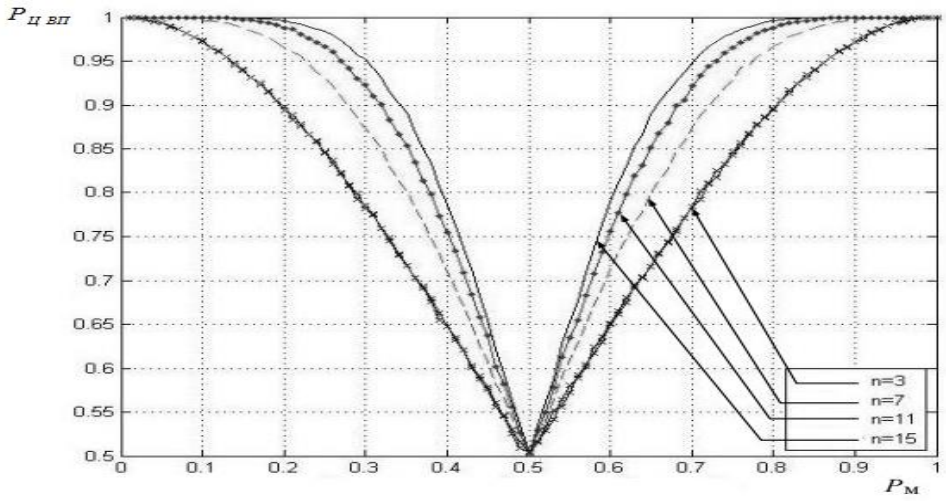

Рис. 4. Результати імітаційного моделювання роботи ВП $P_{Ц\ ВП} = f(P_M)$ для різних значень n.

Для забезпечення цілісності інформації за рахунок організації паралельних незалежних з'єднань між ВД і ВО необхідно вибирати ті з'єднання, у яких відношення $\frac{\ln(1-p_i)}{c_i}$ максимальне.

Висновки

Застосування методу інформаційного резервування і резервування елементів інфраструктури дозволяє забезпечити доступність і цілісність інформації в мультисервісних мережах зв'язку з QoS.

Список використаної літератури

1. Богатырев, В. А. Надежность двухуровневой отказоустойчивой компьютерной системы при дублировании связей между узлами / В. А. Богатырев // Вестн. компьютер. и информ. технологий. – 2009. – № 1. – С. 2–7.

2. Финк, Л.М. Теория передачи дискретных сообщений. Изд. 2-е, переработанное, дополненное. / Л.М. Финк. – М.: Советское радио, 1970 – 728 с.

3. Хорошевский, В.Г. Архитектура вычислительных систем: Учеб. пособие. –2-е изд., перераб. и доп. / В.Г. Хорошевский – М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. – 520 с.

4. Новиков, С. Н. Обеспечение целостности в мультисервисных сетях / С. Н. Новиков, О. И. Солонская // Доклады ТУСУР . – 2009. – № 1(19), ч. 2. – С. 83–85.

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

Надійшла: 25.01.2018 Рецензент: к.т.н. Курченко О.А.