11. Цмоць І., Демида Б. Структури пам'яті з дисципліною доступу FIFO // Вісник ДУ "Львівська політехніка". – 1999. – №386. – С. 21 – 26.
12 Цмоць І.Г., Рашкевич Ю.М., Демида Б.А., Ревич М.Р., Кашем А.М. Паралельна пам'ять систем управління та цифрової обробки і оцінка її основних характеристик // Вестник Харьковского государственного политехнического университета "Системный анализ, управление и информационные технологии". – Харьков, 2000. – Вып.97. – С.79 – 84.
13. Кун С. Матричные процессоры на СБИС. – М.:Мир,1991. – 672 с.
14. Цмоць І.Г. Принципи розробки і оцінка основних характеристик високопродуктивних процесорів на надвеликих інтегральних схемах // Вісник ДУ "Львівська політехніка". – 1998. – №349, – С. 5 – 11.

О. Івахів, Ю. Мочернюк, І. Шигера
Національний університет "Львівська політехніка"

УДК 621.398

ВПЛИВ ЗАВАД НА ПРОПУСКНУ ЗДАТНІСТЬ КАНАЛУ ЗВ'ЯЗКУ ДЛЯ АДАПТИВНОЇ СИСТЕМИ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ

Досліджується вплив завад на пропускну здатність каналу зв'язку та виводяться вирази для похибки відновлення в адаптивних системах передавання інформації.

The effect of false signal on the adaptive data transmission systems communication channel capacity demands and total renovation error estimation are investigated in this paper.

Вступ

Часто електромеханічні виконавчі механізми автоматизованих систем керування працюють в автономному режимі, спілкування з ними здійснюється за допомогою засобів зв'язку, а моменти надсилання керуючого сигналу визначаються на підставі аналізу інформації щодо стану досліджуваного об'єкта [1]. Оскільки об'єкти здебільшого складні та багатофункційні, то для одержання якомога повнішої та об'єктивнішої інформації, придатної до її комп'ютерного опрацювання, використовуються багатоканальні цифрові вимірювальні системи. Водночас, внаслідок дії завад каналу зв'язку на передавані повідомлення можливе спотворення як адресних, так і інформаційних їх

частин, що приводить до втрат суттєвих та появи хибних відліків, спотворення виміряних значень [2]. Часто виявлення спотворених повідомлень та їх витирання здійснюється окремою перевіркою парності кількості розрядів як адресної, так і інформаційної частин повідомлення, що передбачає введення додаткового двійкового розряду. З врахуванням цього в роботі [3] виведено вирази для оцінювання значень сумарних середньоквадратичних похибок відновлення вимірювальних сигналів та побудовано залежності мінімуму пропускної здатності каналу зв'язку від узагальнених параметрів кількох типів адаптивних систем, зокрема й для системи з прогнозуванням нульового порядку та генератором часових позначок.

Формулювання задачі

Оскільки введення надмірних символів дещо підвищує вимоги до швидкодії, а тому при певних умовах навіть адаптивне дискретизування може програвати регулярному [4,5], то доцільно дослідити області оптимального застосування безнадлишкового кодування чи ж використання перевірки парності із подальшим витиранням спотворених відліків, виходячи з критерію мінімуму пропускної здатності каналу зв'язку на прикладі адаптивної системи з прогнозуванням та генератором часових позначок; при цьому синхронізування вважається ідеальним, а серед спотворень двійкових розрядів внаслідок дії завад враховуються лише однократні як найімовірніші.

Безнадлишкове кодування адресної та інформаційної частин

Вираз для середньоквадратичної похибки від дії завад на повідомлення у каналі зв'язку [2]:

$$\delta^2_{кан} = 4\frac{4^{m_i}-1}{4^{m_i}}P + \varepsilon^2 P m_a + 2\frac{4^{m_i}-1}{4^{m_i}}\frac{\lambda^{(i)}_{хв}}{\lambda^{(i)}_{хв}+\lambda_i}, \qquad (1)$$

тут m_a, m_a – розрядність адресної та інформаційної частин повідомлення, відповідно; ε – відносна апертура прогнозування [3]; P – ймовірність спотворення одного двійкового символу; λ_i – інтенсивність потоку відліків i-го джерела ($i = 1, ..., n_c$, де n_c – загальна кількість джерел).

Для інтенсивності потоку хибних відліків, що потрапили в i-е джерело при спотворенні адрес усіх інших джерел сукупності, можна записати [3]

$$\lambda^i_{хв} = \sum_{j=1, j\neq i}^{n_c} \lambda_j P_{ij} = (\lambda_\Sigma - \lambda_i)\frac{m_a P}{2^{m_a}-1}, \qquad (2)$$

де $n_{еф}$ – ефективна кількість джерел сукупності; P_{ij} – ймовірність перетворення адреси j-го джерела на адресу i-го.

Підставляючи (2) в (1) та враховуючи, що $2^{m_i} >> 1$, можна отримати

$$\delta^2_{кан} = 4P + \frac{2}{\frac{n_c-1}{n_{еф}-1}\frac{1}{m_a P}+1} + \varepsilon^2 P m_a. \qquad (3)$$

При цьому вираз для пропускної здатності каналу зв'язку

$$\frac{R}{\omega_\Sigma}=\frac{m_a+m_i}{\sqrt{6\pi}\left(\rho-\frac{1}{K_m}\right)}\sqrt{\frac{1+12\left[\frac{P_в(1+P_в)}{(1+P_в)^2}+Pm_a\right]+2\frac{K_m\rho-1}{n_{еф}^2}}{\delta_{доп}^2-\frac{2P}{\frac{n_c-1}{n_{еф}-1}\cdot\frac{1}{m_a}+P}-4P}}, \tag{4}$$

де ρ – коефіцієнт завантаженості каналу зв'язку ($\rho=0{,}99$); K_m – зведений період позначок часу [2]; $P_в$ – імовірність втрати повідомлення внаслідок переповнення буферного запам'ятовувального пристрою [3] ($P_в=0{,}002$); $\delta_{доп}$ – допустима середньоквадратична відносна похибка відновлення вимірювального сигналу.

Взявши першу похідну по K_m та прирівнявши її до нуля, можна знайти його оптимальне значення, що мінімізує (4)

$$K_{mopt}=\frac{1}{\rho}\cdot\left\{1{,}5+\sqrt{0{,}25+n_{еф}^2\left(1+12\left[\frac{P_в(1+P_в)}{(1-P_в)^2}+Pm_a\right]\right)}\right\}. \tag{5}$$

Безнадлишкове кодування адресної частини

Для цього випадку вираз (3) та значення пропускної здатності каналу зв'язку та оптимального зведеного періоду позначок часу перепишемо так

$$\delta_{кан}^2=\varepsilon^2P(m_a+m_i+1)+\frac{2}{\frac{n_c-1}{n_{еф}-1}\frac{1}{m_aP}+1}, \tag{6}$$

$$\frac{R}{\omega_\Sigma}=\frac{m_a+m_i+1}{\sqrt{6\pi}\left(\rho-\frac{1}{K_m}\right)}\sqrt{\frac{1+12\left[\frac{P_в(1+P_в)}{(1+P_в)^2}+P(m_a+m_i+1)\right]+2\frac{K_m\rho-1}{n_{еф}^2}}{\delta_{доп}^2-\frac{2}{\frac{n_c-1}{n_{еф}-1}\cdot\frac{1}{m_a}+1}}}, \tag{7}$$

$$K_{mopt}=\frac{1}{\rho}\cdot\left\{1{,}5+\sqrt{0{,}25+n_{еф}^2\left(1+12\left[\frac{P_в(1+P_в)}{(1-P_в)^2}+P(m_a+m_i+1)\right]\right)}\right\}, \tag{8}$$

відповідно.

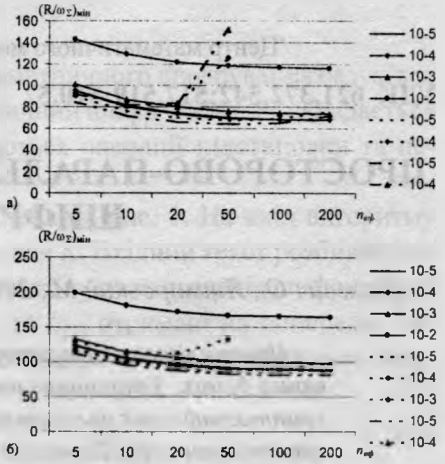
Перевірка на парність із витиранням адресної та інформаційної частин повідомлення

Для цього випадку вирази для пропускної здатності каналу зв'язку та оптимального значення K_m матимуть, відповідно, вигляд [3]

$$\frac{R}{\omega_\Sigma} = \frac{m_a + m_i + 2}{\sqrt{6\pi}\delta_{доп}\left(\rho - \frac{1}{K_m}\right)}\sqrt{1 + 12\left[\frac{P_в(1+P_в)}{(1+P_в)^2} + P(m_a + m_i + 2)\right] + 2\frac{K_m\rho - 1}{n_{еф}^2}}, \qquad (9)$$

$$K_{mopt} = \frac{1}{\rho}\left\{1{,}5 + \sqrt{0{,}25 + n_{еф}^2\left(1 + 12\left[\frac{P_в(1+P_в)}{(1-P_в)^2} + P(m_a + m_i + 2)\right]\right)}\right\}. \qquad (10)$$

На рисунку наведено збудовані залежності пронормованої пропускної здатності каналу від ефективної кількості джерел та ймовірності спотворення $(R/\omega_\Sigma) = f(n_{еф}, P)$ для $m_a = 4$ (а) та $m_a = 9$ (б) при забезпеченні допустимої похибки відновлення $\delta_{доп} = 0.06$ (1%), тут суцільною лінією позначено залежності для адаптивної системи з перевіркою на парність адресної та інформаційної частин повідомлення, штриховою – залежності для системи з безнадлишковим кодуванням адресної частини, а штрих-пунктирною – з безнадлишковим кодуванням адресної та інформаційної частин.



Залежності мінімумів пропускної здатності каналу зв'язку для різних типів адаптивних систем

Висновки

Система з безнадлишковим кодуванням адресної та інформаційної частин найефективніша за критерієм мінімуму пропускної здатності каналу зв'язку при $m_a = 4$: $P = 10^{-5}$, $n_{еф} = 5$ - 120 та $P = 10^{-4}$, $n_{еф} \le 7$, а при $m_a = 9$: $P = 10^{-5}$, $n_{еф} = 5$ - 200. Систему з безнадлишковим кодуванням адресної частини найдоцільніше використовувати для $m_a = 9$, $P = 10^{-4}$, $n_{еф} = 5 - 90$ та $P = 10^{-3}$, $n_{еф} = 5 - 12$. Для решти значень m_a, P та $n_{еф}$ оптимальною за цим критерієм є система з перевіркою парності та витиранням повідомлення при спотворенні адресної чи інформаційної його частин. Проте із зростанням кількості джерел, що опрацьовуються системою, ефективність такого кодування зменшується і водночас звужується область застосування.

1. Ильясов Б.Г., Старцев Ю.В., Головацкий К.Э., Альмухамедов Р.Р., Белалов Б.М. Автономные наземные транспортные средства как объекты автоматического управления//Мехатроника. – 2001. – №6. – С. 3 – 5.
2. Ивахив О. В., Карлов А. А., Черкасов В. В. Влияние канала связи на качество передачи непрерывных сообщений в адаптивных системах передачи информации // Изв. ВУЗов: Радиоэлектроника. – Т. 20. – 1977. – С. 12 – 22.

3. Калашников И. Д., Степанов В. С., Чуркин А. В. Адаптивные системы сбора и передачи информации. – М.,1975.
4. Ю. Василик, О. Івахів. Порівняння альтернативних принципів організації абонентського пункту вимірювально-обчислювальної мережі // Вісник ДУ"Львівська політехніка". – 1994. – №283. – С. 66 – 74.
5. Базилевич О., Голдак А., Івахів О., Серкіз А. Дослідження доцільності проектування адаптивної вимірювальної системи // Тези доповідей VI Міжнародної науково-технічної конференції "Контроль і управління в складних системах"(КУСС-2001), Вінниця, 8-12 жовтня 2001 року. – С. 252.

О. Ліскевич, М. Яцимірський*
Національний університет "Львівська політехніка"
*Центр математичного моделювання ІППММ ім. Я.С. Підстригача НАН України

УДК 621.372.542:517.519:510.52

ПРОСТОРОВО-ПАРАЛЕЛЬНІ СТРУКТУРИ АПАРАТНОГО ШИФРУВАННЯ ДАНИХ

Проаналізовано структурні особливості алгоритмів симетричного шифрування даних. Запропоновано новий підхід до побудови просторово-паралельних криптографічних алгоритмів. На його основі розроблено структуру матричного криптопроцесора. Показано можливість досягнення вищої, порівняно з відомими алгоритмами, продуктивності та надійності шифрування даних.

Structural peculiarities of symmetric cryptoalgorithms have been investigated. The new approach to parallel cryptoalgorithms development is proposed. SIMD matrix processor based on the proposed approach is developed. Possibility of cipher reliability and system throughput improvement, comparative to known algorithms, is shown.

1. Вступ

Інформаційні ресурси в наш час не поступаються за вартістю таким традиційним цінностям, як енергія чи сировина. Відповідно гостро стоять задачі захисту інформації [1, 2, 3]. Серед сучасних методів захисту інформації важливе місце посідають криптографічні алгоритми, що поділяються на симетричні та асиметричні [1]. В симетричних криптосистемах один і той же ключ використовується для шифрування та дешифрування. Асиметричні системи використовують два різні ключі. Сучасні системи захисту інформації часто поєднують обидва підходи, наприклад, асиметричні алгоритми для розповсюдження ключів та симетричні – для безпосереднього шифрування даних