10Ш

УДК 621.377;629.735.05

Б.М. Шевчук, В.К. Задірака, С.В. Фраєр
Інститут кібернетики ім. В.М. Глушкова НАН України, м. Київ, Україна
incors@ukr.net

Ефективні методи фільтрації-стиску та захисту інформації в комп'ютерних мережах тривалого моніторингу станів об'єктів

Обгрунтовуються вимоги до способів отримання достовірних даних моніторингу і описуються функціональні характеристики ефективних методів фільтрації-стиску та захисту інформації, які є основою оперативної багатофункціональної обробки даних в моніторингових мережах.

Вступ

Сучасні дослідження в різноманітних галузях науки, промисловості, медицини, телемедицини і спорту вимагають отримання достовірних кількісних оцінок станів стаціонарних, рухомих та віддалених об'єктів, до яких відносяться складні людино-машинні комплекси і системи, технічні об'єкти і технологічні процеси, природні об'єкти і явища, об'єкти екомоніторингу, транспорту, сільськогосподарські об'єкти, біооб'єкти. Тому ефективне вирішення проблем моніторингу станів об'єктів вимагає використання в місцях виникнення інформаційних потоків високоінтелектуальних об'єктних терміналів і абонентських систем комп'ютерних мереж. При цьому обробка даних моніторингу (ДМ) на об'єктах повинна бути багатофункціональною, включаючи фільтрацію і стиск сигналів, визначення інформаційних станів об'єктів, захист даних від підміни та від несанкціонованих користувачів, завадостійке кодування та маскування пакетів інформації, що передаються в шумах каналів зв'язку. Ключовою проблемою обробки даних на об'єктах є оптимізація формування первинних інформаційних потоків для завантаження засобів накопичення даних та каналів зв'язку комп'ютерних мереж достовірною стислою інформацією. Тому актуальною є розробка математичних основ і методів оперативної багатофункціональної обробки та кодування інформації в умовах багатьох обмежень, включаючи обмеження на продуктивність об'єктових обчислювальних ресурсів, часу обробки та обмеження на пропускну здатність мереж зв'язку.

Мета роботи та постановка задачі. Оскільки об'єктові термінали та абонентські системи моніторингових мереж є первинною ланкою, яка визначає інформаційні потоки та завантажує мережеві ресурси тим об'ємом інформації, який підлягає багатоступінчатій обробці, зберіганню та передачі на великі відстані, то надзвичайно важливо організувати комплексну обробку ДМ на об'єктах таким чином, щоб виявити та компактно передати інформативні фрагменти сигналів і зображень, максимально мінімізувавши втрати діагностичної інформації та суттєво зменшивши передачу на верхні рівні моніторингової мережі недостовірної та зашумленої інформації. Тому

метою роботи є обґрунтування та розробка ефективних по швидкодії і точності методів фільтрації, стиску і захисту інформації, що передається від об'єктів моніторингу в мережу. В статті аналізуються вимоги до способів отримання достовірних ДМ та описуються функціональні характеристики методів багатофункціональної обробки аналогових сигналів і зображень з урахуванням внесення мінімальних спотворень у процесі кодування та відновлення відліків огинаючої сигналів. Окрім вирішення проблеми мінімізації інформаційних потоків важливо в темпі обробки даних максимально захистити інформаційні кадри пакетів від підміни та від доступу до них несанкціонованих користувачів. Тому в статті пропонуються комбіновані методи оперативного захисту двійкових даних та маскування пакетів інформації в шумах каналів зв'язку з урахуванням поточних вимог надійної доставки стислої та захищеної інформації абоненту-адресату.

Аналіз та обґрунтування вимог до способів отримання достовірних ДМ

З метою забезпечення ефективного функціонування комп'ютерних мереж тривалого моніторингу станів об'єктів абонентські системи повинні контролювати умови відбору ДМ, оперативно оцінювати якість введених аналогових сигналів (АС), їх достовірність і на основі отриманих даних здійснювати адаптивну по складності, точності і швидкодії первинну обробку ДМ. Більш ефективнішою є обробка ДМ в залежності від визначеного інформаційного стану об'єкта [1], [2] на основі апертурного контролю відповідних кореляційних, спектральних, статистичних, хаотичних характеристик сигналів. В роботі [1] показано, що первинні інформаційні потоки суттєво залежать від вимог до метрологічних характеристик апаратури підсилення, аналогової фільтрації і аналого-кодового перетворення сигналів. Зменшення інформаційних потоків без втрат по точності відновлення огинаючої кривої сигналів вимагає використання складних та дорогих ФНЧ, АЦП і ускладнених методів цифрової фільтрації, стиску інформації та апроксимації відліків сигналів. Це пов'язано з тим, що частота опиту сигналів є функцією багатьох параметрів. Для багатоканального пристрою введення і перетворення інформації можна записати такий вираз:

$$f_{on}^{N} = f\left(N, f_{max}^{m}, K_{ф}^{m}, P^{m}, n^{m}, A_{max}^{m}, A_{min}^{m}, q_{max}^{m}, \delta_{s}^{m}\right), \qquad (1)$$

де f_{on}^{N} – частота опиту N – канального АЦП, f_{max}^{m} – максимальна частота m-го сигналу з найбільш високочастотною складовою, $K_{ф}^{m}$ – коефіцієнт степеня підвищення частоти дискретизації m-го сигналу в залежності від типу P^{m} і порядку n^{m} ФНЧ, значення розмаху пульсацій A_{max}^{m} у смузі пропускання ФНЧ та значення подавлення A_{min}^{m} сигналу в смузі подавлення ФНЧ, q_{max}^{m} – максимальна кількість двійкових біт при кодуванні m-го сигналу, $\delta_{s}^{m} \approx \delta^{m}{}_{ni} + \delta^{m}{}_{n} + \delta^{m}{}_{ФНЧ} + +\delta^{m}{}_{АЦП} + \delta^{m}{}_{a}$, $\delta^{m}{}_{s}$ – сумарна відносна похибка всього тракту введення та обробки інформації m-го каналу, $\delta^{m}{}_{ni}$ – похибка первинного перетворювача інформації m-го каналу, $\delta^{m}{}_{n}$ – похибка засобів підсилення m-го сигналу, $\delta^{m}{}_{ФНЧ}$ – похибка ФНЧ, $\delta^{m}{}_{АЦП}$ – похибка АЦП, $\delta^{m}{}_{a}$ – похибка способу апроксимації у процесі відновлення огинаючої m-го сигналу.

Таким чином за точну і достовірну інформацію про амплітудо-частотні та фазові характеристики сигналів, які підлягають тривалому контролю, необхідно «платити» формуванням суттєво підвищених інформаційних потоків, використовуючи точні та складні апаратні засоби. Дослідження показали [1], що в порівнянні з частотою дискретизації за Котельниковим на практиці величину $f_{оп}$ необхідно вибирати в $K_ф$ разів більшою згідно з виразом $f_{оп} = 2 \cdot K_ф \cdot f_{max}$, де $K_ф \geq 6-8$. При виконанні точних вимірювань, коли $q_{max} \geq 12$, для забезпечення мінімальних потоків даних доцільно використовувати сигма-дельта-АЦП.

З метою виявлення, класифікації та відображення достовірних і недостовірних ділянок сигналів у процесі фільтрації і стиску сигналів доцільно визначати та компактно кодувати ділянки сигналів з різним вхідним співвідношенням сигнал/шум ($[с/ш]_{вх}$). Опосередковано якість введених даних, степінь їх «зашумленості» можливо проконтролювати по рівню високочастотних шумів та дрейфу ізолінії. Аналіз умов отримання достовірних даних моніторингу показує, що операції фільтрації і стиску є взаємозалежними або виконуються шляхом реалізації базових перетворень інформації. Прикладами таких процедур є методи фільтрації і стиску АС на основі узагальнених ортогональних Фур'є і вейвлет-перетворень [3-5]. Для виявлення характерних спотворень, які виникають при використанні поширених методів фільтрації сигналів і зображень, проаналізуємо алгоритми фільтрації АС на основі ковзкого усереднення, медіанної фільтрації та фільтрації на основі ортогональних перетворень (дискретно-косинусного перетворення (ДКП), вейвлет-перетвореннь з використанням вейвлетів Хаара, Добеші 8, 12 та 14). Проаналізуємо фільтрацію АС з позицій забезпечення мінімальних спотворень огинаючої сигналу. Аналіз здійснимо з використанням теоретичного сигналу з відомими інформативними та шумовими складовими при $K_ф = 8$ (рис. 1, а), де верхня крива – сигнал з шумами, середня – сигнал без шумів, нижня – шумова складова. На рис. 1 стрілками вказується місцезнаходження імпульсних завад, а на рис. 1 в – з верхня крива – сигнал без шумів, середня крива – відфільтрований сигнал. Фільтрація АС в режимі обчислення ковзкого середнього (рис. 1 ,б) вимагає адаптивного підбору довжини вікна усереднення і усереднює спотворені (зашумлені) відліки АС, що призводить до появи недостовірних коливань у вихідному сигналі. Враховуючи простоту обробки даних, ковзке згладжування доцільно здійснювати на практично чистих ділянках, а також на ділянках з шумами для приблизного визначення місцезнаходження екстремумів. Медіанна фільтрація (МФ) ґрунтується на операції упорядкування відліків у вікні (рис. 1, в) та на визначенні центрального відліку $X_i^ф$. Недоліком МФ є спотворення форми сигналу на ділянках з екстремумами. Позитивною рисою ДКП [6] є якісне відновлення амплітудних значень відліків АС при реалізації операцій фільтрації і стиску шляхом відкидання високочастотних та низькорівневих коефіцієнтів перетворення (рис. 1, г). Проте оскільки реальні сигнали складаються з різних періодичних та хаотичних компонент, то таких спотворень при використанні ДКП може бути багато. Тому на ділянках вхідного сигналу з різкими переходами огинаючої з шумами після фільтрації на вихідному сигналі появляються значні спотворення форми кривої, які тим помітніші, чим більші амплітудні значення імпульсних завад. В порівнянні з ДКП-фільтрацією більш ефективною є фільтрація на основі дискретного вейвлет-перетворення (ДВП) [3], [5]. Найбільш швидкодіючою фільтрацією з ДВП є використання вейвлетів Хаара (рис. 1, д), а для більш точного

відновлення огинаючої кривої АС доцільно використовувати більш складні вейвлети, наприклад, Добеші 8 (рис. 1, е), Добеші 12 (рис. 1, ж) або Добеші 14 (рис. 1, з). Проте для оптимального відновлення огинаючої АС при використанні ДВП необхідно адаптивно підбирати базисні функції ДВП [7], [8], які за формою максимально подібні до вхідного сигналу. Це підтверджується вихідними сигналами (рис. 1, е – з) після обробки АС з використанням ДВП.

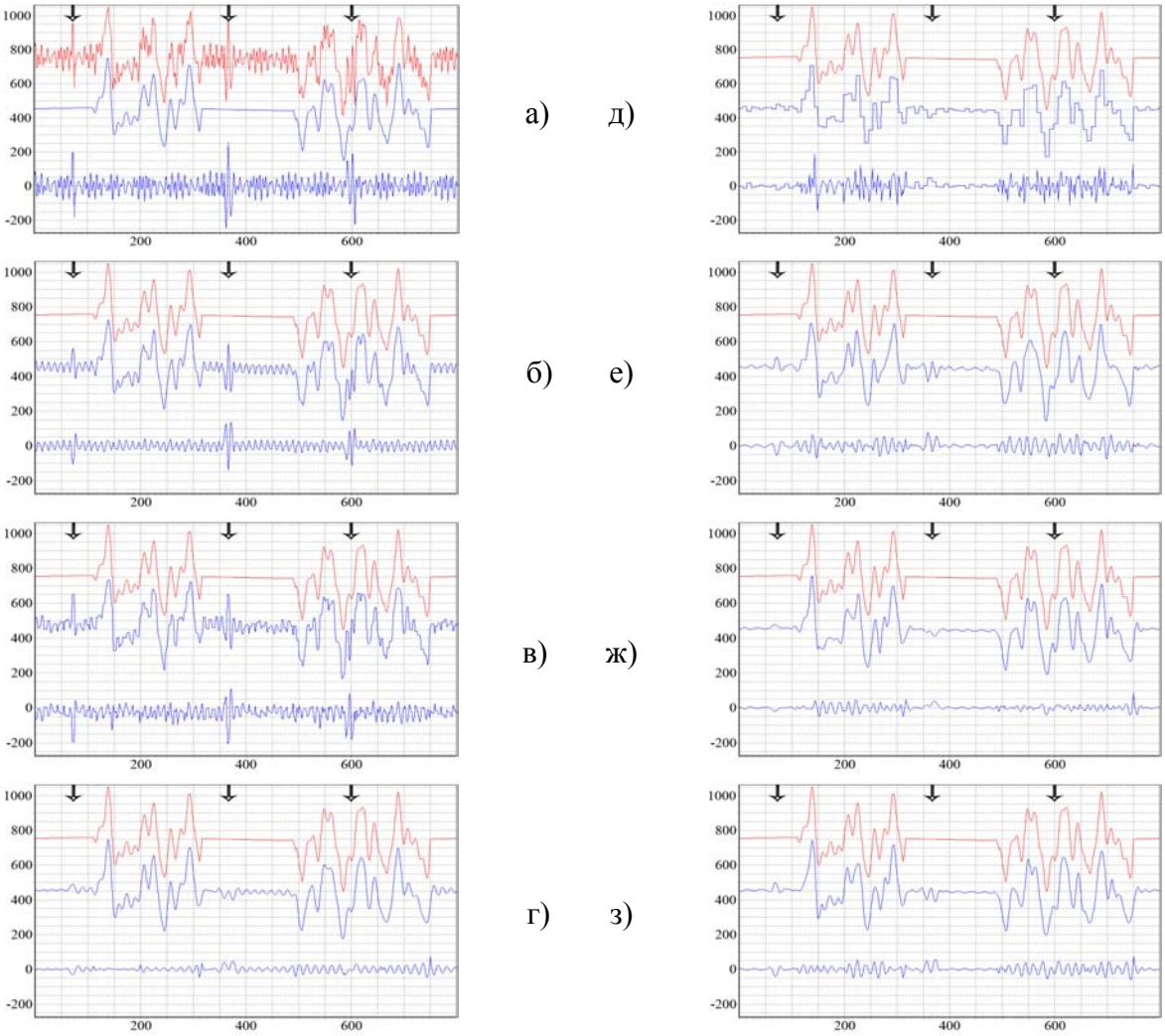

Рисунок 1

Аналіз вимог до способів отримання достовірних відліків АС показує, що при $q_{max} \geq 10$ частоту опиту сигналу потрібно вибирати в $K_ф$ разів більшою за частоту дискретизації за Котельниковим, де $K_ф \geq 6-8$ [1]. Дослідження вихідних сигналів поширених методів фільтрації показують, що кожен з методів вносить відповідні характерні спотворення, які суттєво залежать від величини $[с/ш]_{вх}$, характеристик базису та форм базисних функцій [8]. Оскільки фільтрація і стиск сигналів є взаємозалежними, то доцільно виконувати спільну операцію фільтрації-стиску сигналів, яка враховує їх стан зашумленості.

Функціональні характеристики ефективних методів фільтрації-стиску аналогових сигналів

Оскільки одним із основних завдань оперативної обробки ДМ на об'єктах є мінімізація та формування достовірних потоків інформації, то ключовим завданням для об'єктових систем є фільтрація АС з наступним виконанням операцій стиску та захисту компактних даних. При цьому коефіцієнт стиску аналогових сигналів суттєво залежить від динамічних характеристик огинаючої сигналів, тому операції фільтрації і стиску сигналів доцільно виконувати як спільний процес. З метою розробки ефективних методів фільтрації стиску сигналів обґрунтуємо основні складові операції фільтрації-стиску сигналів.

Ефективним способом визначення величини $[\text{с}/\text{ш}]_{\text{вх}}$ є аналіз рівня високочастотних та низькочастотних шумів (дрейфу ізолінії сигналу) на основі аналізу поточних приростів відліків сигналу. Оскільки низькочастотний дрейф ізолінії сигналу суттєво не впливає на величину потоків даних, то степінь їх «зашумленості» доцільно проконтролювати по рівню високочастотних шумів. При цьому на ділянках, де спостерігаються значні шуми, після фільтрації слід очікувати спотворення форми кривої. Тому на цих ділянках доцільно використовувати спрощені та швидкодіючі методи фільтрації, а для зменшення інформаційних потоків відліки вихідного сигналу доцільно кодувати більш стисло, тобто меншою кількістю біт. Найпростішим і швидким способом визначення степеня зашумленості ділянок сигналів, яка опосередковано характеризується вхідним співвідношенням сигнал/шум $[\text{с}/\text{ш}]_{\text{вх}}$, є обчислення поточної різниці $\Delta X_i^{ш1} = \left| X_i^{ш1} - X_{i-1}^{ш1} \right|$ між сусідніми відліками вхідного (зашумленого) сигналу. Шляхом порівняння величини $\Delta X_i^{ш1}$ з відповідними пороговими величинами $P_1, P_2, \ldots, P_s$ визначається поточний стан зашумленості ділянки сигналу, де s – кількість станів степеня зашумленості сигналу. Найточніше степінь зашумленості відліків сигналів визначається шляхом порівняння величини $\Delta X_{\text{i}}^{\text{ш}2} = \left| X_i^{ш} - X_i^{ф} \right|$ з відносними величинами оперативно відфільтрованих ковзким способом відліків $X_i^{ф}$. Прикладом класифікації станів зашумленості сигналів є визначення таких чотирьох станів:

$$
\begin{aligned}
&\text{«11» (суттєво зашумлена ділянка)} - \Delta X_{\text{i}}^{\text{ш}2} \geq P_1,\ P_1 = X_{\text{i}}^{\text{ф}}/4,\\
&\text{«10» (зашумлена ділянка)} - P_2 \leq \Delta X_{\text{i}}^{\text{ш}2} < P_1,\ P_2 = X_{\text{i}}^{\text{ф}}/8,\\
&\text{«1» (менш зашумлена ділянка)} - P_3 \leq \Delta X_{\text{i}}^{\text{ш}2} < P_2,\ P_3 = X_{\text{i}}^{\text{ф}}/16,\\
&\text{«00» (практично чиста ділянка)} - P_4 \leq \Delta X_{\text{i}}^{\text{ш}2} < P_3,\ P_4 = X_{\text{i}}^{\text{ф}}/32.
\end{aligned}
\qquad (2)
$$

Таким чином для реалізації фільтрації-стиску сигналів на першому етапі оперативної обробки відліків сигналів визначаються ділянки з різним степенем зашумленості, які у свою чергу кодуються різною достовірною кількістю біт $q_{\text{д}} = \text{f}\left([\text{с}/\text{ш}]_{\text{вх}}\right)$. Для прикладу відліки ділянки з кодом $[\text{с}/\text{ш}]_{\text{вх}}$ «11» кодуються з $q_{\text{д}} = 7-8$ біт, ділянці з кодом «10» відповідають $q_{\text{д}} = 8-9$ біт, ділянці з кодом «01» відповідають $q_{\text{д}} = 9-10$ біт, ділянці з кодом "00" відповідають $q_{\text{д}} = 11-12$ біт.

Згідно з результатами дослідження спотворень форми кривої АС при використанні простих методів фільтрації в режимі обчислення ковзкого середнього або при обчисленні медіани похибки фільтрації суттєво залежать від вибору оптимального вікна усереднення $l_{опт} = f(К_ф, \Delta^ф_{мах})$, де $\Delta^ф_{мах}$ – максимальна величина приростів сусідніх відліків $X_i^ф$ на ділянці. При цьому для зменшення спотворень форми огинаючої сигналу доцільно попередньо визначити околиці з екстремальними відліками, амплітудні значення яких можуть бути спотворені завадами. Маючи інформацію про поточну величину $[с/ш]_{вх}$, $l_{опт}$ в подальшому здійснюється більш точна адаптивна фільтрація з метою отримання достовірних відліків $X_i^ф$. В залежності від результатів попереднього аналізу достовірності вхідних даних на більш зашумлених відрізках чи ділянках сигналів реалізуються простіші та швидкодіючі алгоритми фільтрації, а на менш зашумлених ділянках здійснюються більш складніші і точніші алгоритми фільтрації сигналів.

Стиск відфільтрованих відліків ґрунтується на методах визначення і кодування суттєвих відліків (СВ) та несуттєвих відліків (НВ) [9], при цьому СВ кодуються кодом $T_i\{X_i\}$, де $T_i = 1$ – біт ознаки суттєвості відліку сигналу, $\{X_i\}$ – двійковий код суттєвого відліку, який може бути повнорозрядним або різницевим. НВ кодуються одним бітом $T_i = 0$. Одним із варіантів кодування послідовності НВ є формування коду $(T_i = 0)(p_i)$, де $p_i = \lceil \log_2 K_ф \rceil$, $\lceil \cdot \rceil$ – ознака цілої, взятої до більшої. До суттєвих відліків обов'язково слід віднести екстремальні значення відфільтрованого сигналу. Аналіз відфільтрованих сигналів показує, що їх огинаючу утворюють послідовності наростаючих, спадаючих і горизонтальних ділянок сигналу, які повторюються в різних комбінаціях. Наростаюча ділянка характеризується позитивними послідовностями різниць між сусідніми відліками відфільтрованого сигналу $\Delta X_i^ф$, спадаюча – негативними послідовностями $\Delta X_i^ф$, а горизонтальна – нульовими $\Delta X_i^ф$. Дослідження швидко-діючих ковзких методів фільтрації сигналів показали, що на вихідних сигналах зустрічаються короткотривалі коливання і зміни, при цьому тривалості таких відрізків є меншими за півперіод інформативної складової сигналу з частотою f_{max}. З метою економії часу обробки інформації та уникнення зайвих операцій кодування недостовірних СВ після отримання відфільтрованих відліків на інтервалі $T_{обр}$ доцільно виконувати наступні дії:

1) шляхом аналізу величин $\Delta X_i^ф$ виявляються достовірні ділянки (наростаючі, спадаючі, горизонтальні), тривалість яких $t_g \geq K_ф \cdot t_{оп}$, де $t_{оп} = 1/f_{оп}$ – інтервал опиту (дискретизації) сигналу, тобто достовірною є ділянка, якій відповідають $K_ф$ однакових ознак («+», «–», «0») приростів $\Delta X_i^ф$;

2) відліки, які знаходяться на стику достовірних ділянок, є суттєвими і кодуються повнорозрядним двійковим кодом відповідно до такої послідовності службових і інформативних бітів $(T_i = 1)(K_i = 1)\{X_i\}$, де K_i – ознака виду кодування СВ ($K_i = 1$ – код $\{X_i\}$ є повнорозрядним, $K_i = 0$ – код $\{X_i\}$ є різницевим, тобто $\{\Delta X_i\}$);

3) на ділянках, тривалістю $t_{нд} < K_ф \cdot t_{оп}$, та на тривалому інтервалі, який утворюють різнотипні недостовірні ділянки, через кожні $N_{нд} < K_ф$ визначається середнє значення відліків, яке відповідає СВ;

4) на достовірних ділянках здійснюється пошук групи відліків, які знаходяться в околиці точки зміни опуклості кривої шляхом апертурного порівняння сусідніх різниць $\Delta X_i^ф$, тобто для виявлення заданих дослідником відхилень сигналу від лінійних змін аналізуються три сусідні відліки $X_{i-1}^ф, X_i^ф, X_{i+1}^ф$ та визначаються поточні різниці $\Delta X_i^ф = X_i^ф - X_{i-1}^ф$, $\Delta X_{i+1}^ф = X_{i+1}^ф - X_i^ф$, на основі яких формуються булеві змінні ознак суттєвості відліку $X_{i-1}^ф$:

$$T_{i-1} = \begin{cases} 1, \left|\Delta X_{i+1}^{ф} - \Delta X_i^{ф}\right| > \gamma \\ 0, \left|\Delta X_{i+1}^{ф} - \Delta X_i^{ф}\right| \le \gamma \end{cases}, \qquad (3)$$

де $\gamma = f([с/ш]_{вх})$ – величина апертурного відхилення суттєвих відліків $X_i^ф$, які кодуються як група сусідніх СВ.

Оскільки реальні сигнали, як правило, є нелінійними то для їх точного відновлення при спрощеному підході визначення СВ на основі апертурного аналізу поточних різниць згідно з нерівністю (3) необхідно уникати формування тривалих послідовностей НВ. Тому в процесі стиску сигналів через кожні m НВ доцільно формувати черговий СВ, де $m \ge K_ф$. З метою мінімізації інформаційних потоків та спрощення обчислювальних операцій в процесі фільтрації-стиску АС послідовність обробки та кодування потоків вихідних даних доцільно визначати та здійснювати в залежності від степеня зашумленості ділянок сигналів та на основі даних оперативного визначення динамічних характеристик ділянок. Відповідно обробка недостовірних та зашумлених вхідних даних повинна здійснюватись при зменшених частотах опиту сигналів та з використанням мінімальної кількості спрощених операцій. Тому після дискретизації сигналів з частотою $f_{оп} = 2 \cdot K_ф \cdot f_{мах}$, визначення поточного коду $[с/ш]_{вх}$, величини $\Delta_i^ф$ на «суттєво зашумлених» та «зашумлених» ділянках доцільно проріджувати вибірку відліків сигналів, вибравши частоту опиту $f_{оп} = 2 \cdot f_{мах}$. На «менш зашумлених» та «практично чистих» ділянках здійснюється точне визначення амплітудно-часових характеристик екстремумів та границь ділянок. Тому після визначення відповідних кодів $[с/ш]_{вх}$ та реалізації попередньої оперативної фільтрації відліків поточної ділянки шляхом аналізу знаків величин $\Delta X_i^ф$ визначаються місцезнаходження сусідніх екстремумів та їх околиць, тривалістю $l_е = 2 \cdot l_{кс}$, з центральним відмінком, якому відповідають визначені амплітудно-часові параметри екстремуму, де величина $l_{кс}$ може бути вибраною мінімальною (4 – 5 відлік) або визначатись адаптивно з урахуванням того, що $l_{кс} = f(\Delta_i^ф)$. Оперативне визначення величини $\Delta_i^ф$ дозволяє організувати адаптивну обробку сигналів, що є основою для

більш точного та компактного кодування відліків сигналів. Таким чином на ділянках з екстремумами виявляються околиці екстремумів з метою більш точнішого пошуку параметрів екстремумів, які знаходиться в шумах. Поза межами ділянки l_e здійснюється адаптивна медіанна фільтрація, а на інтервалі l_e, для уникнення спотворень, притаманних МФ, реалізується фільтрація з обчисленням ковзкого середнього, наприклад, на «практично чистих» ділянках. З метою реалізації оперативної фільтрації-стиску АС крайні відліки (початок і кінець) ділянки l_e кодуються як СВ, а проміжні відліки є НВ. У процесі кодування в службовій інформації, що відноситься до відрізка з пошуком параметрів екстремуму, поміщається інформація про необхідність виконання даної операції при відновленні форми огинаючої сигналу. Пошук місцезнаходження екстремуму визначається методом перетину протилежних за динамікою ділянок.

З метою реалізації ефективного, адаптивного і компактного кодування суттєвих і несуттєвих відліків сигналу на інтервалі обробки даних $T_{обр}$ визначаються характерні за довжиною відрізки або ділянки сигналу, стисла інформація яких супроводжується службовими даними про вибрану величину q, кодом L_i довжини відрізка чи ділянки, кодом M_i вибраного методу стиску та способів адаптації, кодами визначеного вхідного співвідношення $[с/ш]_{вх}$ та виявлених величин динамічних характеристик відліків сигналу на відрізку або ділянці. Відрізок утворюють послідовності ділянок, кожна з яких починається та закінчується екстремумами, які кодуються СВ повнорозрядними (СВП). Згідно з алгоритмом фільтрації-стиску в ідеальному випадку відрізок утворюють ділянки, які знаходяться між сусідніми глобальними екстремумами, і в залежності від величини $T_{обр}$ відрізок починається та завершується СВП. Кількість можливих достовірних ділянок на інтервалі $T_{обр}$ $K_д = M / K_ф$, тому довжина ділянки кодується $k_д$ – бітовим кодом, де $k_д = \lceil \log_2 K_д \rceil$. В реальних умовах оперативно профільтрований відрізок сигналу можуть утворювати: 1) тривалі наростаюча, спадаюча або горизонтальна ділянки, довжиною $l_д = T_{обр}$; 2) послідовності достовірних ділянок; 3) послідовності достовірних та недостовірних ділянок; 4) послідовності недостовірних ділянок. З метою ефективного кодування відрізків сигналів перелічені послідовності ділянок кодуються зі службовою інформацією, яка характеризує динаміку сигналів, степінь їх зашумленості та вказує на попередньо вибрані методи кодування, способи та параметри адаптації при формуванні стислих двійкових послідовностей СВП, СВ різницевих (СВР) і НВ. Саме за рахунок оперативного визначення динамічних характеристик сигналів та формування короткої службової інформації, яка розміщується попереду стислого інформаційного кадру всього відрізка або окремих ділянок, досягається адаптивний підбір параметрів q_{max}, $f_{опт}$ і Δq, що визначають та впливають на величину інформаційних потоків.

Таким чином, на інтервалі $T_{обр}$ з моменту команди «Пуск» здійснюється визначення степеня зашумленості відліків сигналу і на основі отриманих даних приймається рішення про виявлені типи послідовностей ділянок, що, у свою чергу, дозволяє організувати кодування службової інформації та вибрати відповідні методи стиску та способи адаптації при формуванні стислих двійкових послідовностей відліків сигналу. Слід зазначити, що мінімальна тривалість відрізку або ділянки, для

яких формується службова інформація, досягає величини $l_{min} \geq b \cdot K_ф$, де $b \geq 1$. Тому можливі такі характерні варіанти класифікації типів ділянок та способів кодування службової інформації:

– при виявленні на інтервалі $T_{обр}$ тривалої наростаючої, спадаючої або горизонтальної ділянки (відрізок 1-го типу) або при наявності послідовності недостовірних ділянок (відрізок 4-го типу) вся службова інформація формується для даного відрізка;

– при виявленні послідовності достовірних ділянок (відрізок 2-го типу) або при виявленні на інтервалі $T_{обр}$ хоча б однієї короткої ділянки довжиною $l_д < l_{min}$ серед ділянок з довжиною $l_д \geq l_{min}$ (відрізок 3-го типу), вся службова інформація розбивається на загальну (для всього відрізка) та на локальну (для кожної ділянки).

В залежності від вибраних методів стиску та способів адаптації не виключається можливість формування локальної службової інформації для послідовностей недостовірних ділянок, при цьому необхідна більш детальна обробка ділянок, включаючи повторну фільтрацію та виявлення околиць екстремумів.

До загальної службової інформації, яка розміщується попереду стислого інформаційного кадру відрізка, відноситься:

– (L_i) – l-бітовий код тривалості поточного відрізка сигналу, цей код може повідомляти про кількість відліків на відрізку або про кількість СВП;

– (q_{max}) – максимальний код кількості бітів величини $\{X_i\}$ для СВ;

– (t_i) – 2-бітовий код типу відрізка;

– (C_i) – біт ознаки місцезнаходження службової інформації, яка відноситься до всього відрізка $(C_i = 0)$ або до кожної із ділянок відрізка $(C_i = 1)$;

– (S_i) – s-бітовий код визначеного вхідного співвідношення сигнал/шум;

– (D_i) – d-бітовий код визначених динамічних характеристик відрізка або ділянок. В залежності від вибраного методу стиску та способу адаптації цей код відповідає визначеній максимальній величині приростів оперативно відфільтрованого сигналу $(\Delta_i^ф, \Delta q_{max})$;

– $(K_д)$ – k-бітовий код кількості ділянок на відрізку тривалістю $T_{обр}$;

– (M_i) – m-бітовий код вибраного методу стиску та параметрів адаптації. Цей код деталізує вибрані способи стиску, визначення величин $[с/ш]_{вх}$, вибору $f_{оп}$, способів кодування СВ і НВ та формування службової інформації;

До локальної службової інформації, яка розміщується попереду стислого інформаційного кадру ділянки, відносяться коди (S_i), (D_i) та біти (R_i) і (E_i), де (R_i) – біт ознаки достовірної ділянки $(R_i = 0)$ та недостовірної ділянки $(R_i = 1)$, (E_i) – біт ознаки відновлення відліків околу екстремуму ($E_i = 0$ – необхідність відновлення відліків околу екстремуму, $E_i = 1$ – відсутність відновлення відліків екстремуму). Слід відмітити, що на основі загальної або локальної службової інформації (на основі значень кодів (S_i) і (D_i)) задається мінімально допустима частота опиту сигналу відрізків та ділянок.

Таким чином, стислі послідовності відрізків кодуються біт-орієнтовними інформаційними кадрами, які супроводжуються службовою інформацією, наприклад в такому вигляді: $\{CI_в^1\}\{IK_в^1\}\{CI_в^2\}\{IK_в^2\}...\{CI_в^i\}\{IK_в^i\}...\{CI_в^m\}\{IK_в^m\}$, де $\{CI_в^i\}$ –

службова інформація і-го відрізку сигналу, $i = 1,...,m$, m – максимальна кількість відрізків сигналу, $\{IK_в^i\}$ – інформаційний кадр і-го відрізка сигналу. Для надійного зберігання та відновлення стислих масивів даних кожний блок даних супроводжується відповідною службовою інформацією та байт-орієнтовними послідовностями, які рідко або зовсім не зустрічаються в службових даних та інформаційних кадрах відрізків сигналів. При кодуванні послідовності достовірних ділянок (відрізок 2-го типу) чи послідовностей достовірних і недостовірних ділянок (відрізок 3-го типу) інформаційний кадр і-х відрізків $\{IK_в^i\}$ кодується наступним чином: $\{CI_в^{1,i}\}\{(CI_д^{1,i})(IK_д^{1,i})(CI_д^{2,i})(IK_д^{2,i})...(CI_д^{j,i})(IK_д^{j,i})... ...(CI_д^{p,i})(IK_д^{p,i})\}$, де $(CI_д^{j,i})$ – службова інформація j-ї ділянки і-го відрізку, $(IK_д^{j,i})$ – інформаційний кадр j-ї ділянки і-го відрізку, $j = 1,...,p$, p – максимальна кількість ділянок і-го відрізка.

Захист інформаційних кадрів та маскування пакетів інформації в каналах зв'язку

Для організації дистанційного моніторингу станів об'єктів найбільшого розповсюдження отримали моноканальні комп'ютерні мережі, в яких об'єктові абонентські системи і термінали передають пакети інформації до центральної станції в режимі централізованого або децентралізованого управління передачею даних по моноканалу. Функціонування моноканальних (безпровідникових, коаксіальних, провідникових) мереж ґрунтується на передачі інформації зі зворотнім зв'язком, тобто в моноканалі спостерігаються послідовності пакетів інформації $ІП_i - ПК_i - ІП_j - ... - ІП_m - ПК_m$, які відносяться до різних абонентів моноканальної мережі (i, j, m – номери абонентів мережі), $ІП_i$ – інформаційний пакет і-го абонента, $ПК_i$ – пакет-квитанція для і-го абонента, що передається від абонента-адресата, наприклад від центральної станції (ЦС). Ефективний захист інформації в моніторингових мережах ґрунтується на управлінні роботою об'єктових АС центральною станцією мережі [10], при цьому кожен абонент мережі володіє секретним ключем (СК) та формує криптостійкі псевдовипадкові послідовності (ПВП), які є функцією СК і одноразово формуються для кожного інформаційного кадру (ІК) пакета для виконання операцій гаміювання та псевдохаотичного перемішування зашифрованих ІК. Також формуються криптостійкі хеш-функції ІК у вигляді CRC-кодів [11], [12]. Окрім захисту інформації на рівні ІК здійснюється захист та маскування даних, що підлягають передачі по каналах зв'язку шляхом формування псевдохаотичних шумоподібних пакетів інформації. Для пояснення суті даної операції розглянемо рис. 2, на якому показані вихідні сигнали двох кореляційних приймачів шумоподібних сигналів (ШПС) з базами B=31, які характеризують різний степінь «зашумленості» каналу зв'язку: а) M=0 (канал зв'язку «чистий»); б) M=7 (канал частково «зашумлений»); в) M=11 (канал зв'язку сильно «зашумлений»); г) M=12; д) M=13, де M відповідає кількості спотворених чи невірно прийнятих елементів ШПС. Відповідно для додаткового захисту і маскування даних в каналі зв'язку доцільно двійкові послідовності ІК передавати у вигляді випадково змінних за тривалістю і частково спотворених ШПС, при цьому ЦС для кожного пакета даних відповідного абонента повинна володіти інформацією про місцезнаходження поточних основних піків кореляційної функції.

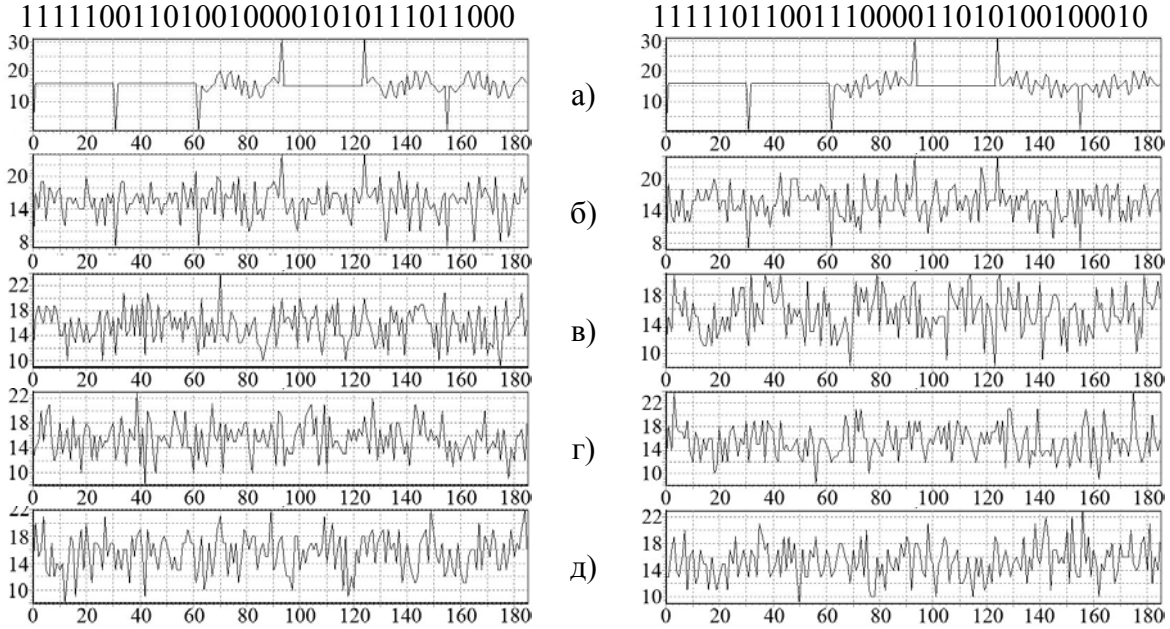

Рисунок 2

Для надійного забезпечення заданого степеня захисту інформації в моніторингових мережах кожен абонент, окрім СК, має узгоджені з ЦС масиви ПВП, які є кодовими ключами генераторів для формування шифру з одноразовим ключем. З метою періодичної зміни абонентських СК доцільно використовувати асиметричні методи захисту інформації [13], [14] при роздачі абонентам ключів центральною станцією.

Висновки

Ефективне функціонування моніторингових мереж ґрунтується на реалізації об'єктовими терміналами і системами багатофункціональної обробки ДМ, включаючи фільтрацію-стиск АС, захист та маскування ІК. З метою отримання достовірних відліків АС при $q_{max} \geq 10$ частота дискретизації сигналу вибирається в $2K_ф$ більшою за f_{max}, де $K_ф \geq 8$. Для прискорення обробки даних та підвищення коефіцієнту стиску АС в процесі фільтрації-стиску доцільно враховувати стан зашумленості вхідної інформації та поточні динамічні характеристики АС. Основою захисту інформації з заданим степенем криптостійкості є поєднання шифрування з одноразовим ключем ІК та маскування інформації в каналі зв'язку шляхом формування псевдохаотичних пакетів інформації. Періодична зміна СК здійснюється з використанням асиметричних методів та засобів їх реалізації.

Література

1. Шевчук Б.М. Методи визначення та відображення показників інформаційних станів об'єктів тривалого моніторингу // Комп'ютерні засоби, мережі та системи. – 2005. – № 4. – С. 78-85.
2. Шевчук Б.М. Методы оперативной обработки сигналов и вычисления показателей состояний объектов в процессе их длительного дистанционного мониторинга // Компьютерная математика. – 2005. – № 1. – С. 94-103.
3. Дьяконов В.П. Вейвлеты. От теории к практике. – М.: СОЛОН – Р, 2002. – 448 с.

4. Иванов В.Г., Любарский М.Г., Ломоносов Ю.В. Фурье- и вейвлет-анализ изображений в плоскости JPEG-технологий // Проблемы управления и информатики. – 2004. – № 5. – С. 111-124.
5. Уэлстрид С. Фракталы и вейвлеты для сжатия изображений в действии. – М.: Триумф, 2003. – 320 с.
6. Яцимірський М.М. Швидкі алгоритми ортогональних тригонометричних перетворень. – Львів: Академічний експрес, 1997. – 219 с.
7. Наконечний А.Й. Теорія малохвильового WAVELET перетворення та її застосування. – Львів: Фенікс, 2001. – 278 с.
8. Классические ортогональные базисы в задачах аналитического описания и обработки информационных сигналов / Ф.Ф. Дедус, Л.И. Куликова, А.Н. Панкратов и др. / Под ред. Ф.Ф. Дедуса. – М.: Издательский отдел факультета ВМиК МГУ им. М.В. Ломоносова, 2004. – 172 с.
9. Шевчук Б.М. Оптимізація процесів введення і оперативного оброблення сигналів в комп'ютерних мережах дистанційного моніторингу станів об'єктів дослідження і керування. Оброблення сигналів і зображень та розпізнавання образів // Праці Сьомої Всеукр. міжнар. конф. – Київ: Укр. асоц. з обробл. інформ. та розпізн. образів, 2004. – С. 263-266.
10. Шевчук Б.М., Фраер С.В. Защита информации в компьютерных мониторинговых сетях на основе маскирования сжатых данных и передачи псевдослучайных шумоподобных пакетов информации // Компьютерная математика. – 2006. – № 1. – С. 80-87.
11. Асемблер в задачах защиты информации / А.А. Абашеев, И.Ю. Жуков, М.А. Иванов и др. – М.: КУДИЦ-ОБРАЗ, 2004. – 544 с.
12. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 816 с.
13. Задирака В.К., Кудин А.М. Построение программно-аппаратных комплексов арифметики сверхбольших чисел // Компьютерная математика. – 2001. – № 1. – С. 532-541.
14. Задірака В.К., Олексюк О.С. Комп'ютерна арифметика багаторозрядних чисел: Наукове видання. – Київ, 2003. – 264 с.

Б.М. Шевчук, В.К. Задирака, С.В. Фраер

Эффективные методы фильтрации-сжатия и защиты информации в компьютерных сетях длительного мониторинга состояний объектов

Обоснованы требования к способам получения достоверных данных мониторинга и описаны функциональные характеристики эффективных методов фильтрации-сжатия и защиты информации, которые являются основой оперативной многофункциональной обработки данных в мониторинговых сетях.

Shevchuk B.M., Zadiraka V.K., Fraier S.V.

Effective Methods of a Filtration-Compression and Protection of the Information in Computer Networks of Long Monitoring Conditions of Objects

Requirements to ways of reception of authentic data of monitoring are proved. Functional characteristics of effective methods of a filtration-compression and protection of the information which are a basis of operative multipurpose data processing in the networks of monitoring are described.

Стаття надійшла до редакції 27.06.2006.