МЕТОДИ Й АЛГОРИТМИ ІНФОРМАЦІЙНИХ СИСТЕМ

УДК 632

Б. Балич, О. Різник, Д. Скрибайло-Леськів
Національний університет "Львівська політехніка"
кафедра автоматизованих систем управління

СИНТЕЗ ПОЛІМОРФНО-ЗАВАДОСТІЙКОГО КОДУВАННЯ НА ОСНОВІ КІЛЬЦЕВОГО МОНОЛІТНОГО КОДУ

Показано можливість застосування нового класу кодуючих систем з використанням комбінаторних числових моделей – монолітних кодів, побудованих на ідеальних кільцевих в'язанках, для вирішення задач поліморфно-завадостійких кодувань за такими критеріями, як підвищення стійкості кодуючої системи та завадостійкості коду від спотворення у фізичному каналі зв'язку. Наведено приклади побудови таких кодів на основі вищезгаданих комбінаторних моделей.

Possibility of application of new class of the encoding systems is shown with the use of combinatorial numerical models – monolithic codes, built on ideal circular bundles, for the decision of tasks polymorphic – antijamming codes after such criteria as an increase of firmness of the encoding system and code antijammingness from distortion in the physical channel of connection. The examples of construction of such codes are resulted on the basis of afore-mentioned combinatorial models.

Вступ

Проблема захисту інформації шляхом її перетворення, що унеможливлює прочитання інформації сторонньою особою, ще кілька десятиліть тому стосувалася тільки військових організацій або була пов'язана зі шпигунськими історіями, а не становила предмет широкого використання. Причиною бурхливого пошуку нових методів кодування, з одного боку, стало використання комп'ютерних мереж, зокрема глобальної мережі Internet, в котрій передаються великі обсяги інформації державного, військового, комерційного та приватного змісту, а з іншого – поява нових потужних обчислювальних засобів, що уможливлює дискредитацію низки кодуючих систем. Зі зростом потужності інформаційних технологій, постала потреба у створенні якісніших кодуючих систем. Якість кодування даних визначається такими показниками, як точність, повнота, захищеність, завадостійкість тощо. Одним із шляхів підвищення якості даних є застосування надлишкового коду. Надлишок інформації використовують в основному для виправлення помилок (такі коди називають завадостійкими) або для забезпечення надійності від несанкціонованого доступу до інформації. Виходячи з останніх досліджень, основним недоліком всіх попередніх алгоритмів кодування є статична незмінність алфавіту кодуючої послідовності; вважають, що для одного варіанта вхідного повідомлення існує тільки одна кодуюча послідовність. Щодо завадостійкості системи, алгоритми котрих також побудовані за принципами використання інформаційної надлишковості, цей метод дає змогу виявляти і виправляти помилки накладанням додаткових умов на сигнали з подальшою перевіркою цих умов на приймальній стороні [1]. Однак це вимагає впровадження спеціальних, часто доволі складних методів перевірки їх виконання.

Виходячи з твердження про те, що кодуючі системи з використанням сучасних алгоритмів не є конкурентоспроможними з погляду захисту інформації, а алгоритми коригування помилок є

громіздкими, виникає запитання: чи можливо створити алгоритм побудови коду з високою здатністю захисту інформації та виправлення великої кількості помилок, з мінімальним рівнем складності реалізації.

Аналіз останніх досліджень

До коригуючих кодів з простими правилами кодування і декодування інформації належить двійковий "монолітний код". Монолітним називається двійковий код, дозволені комбінації якого утворюються зі щонайбільше двох пакетів однойменних символів. Конфігурація таких послідовностей може бути будь-якою, наприклад, набувати вигляду ланцюжка, розгалуженого дерева або кільця. Тому можна говорити про ланцюжкові, кільцеві, гіллясті та інші різновиди монолітних кодів. Важливою перевагою монолітного двійкового коду є висока швидкість виявлення та виправлення помилок, оскільки поява хоча б одного символу "1" серед нулів або символу "0" серед одиниць у прийнятій кодовій комбінації відразу вказує на помилку [2]. Помилка не виявляється лише у тих випадках, коли хибний сигнал виникає в першому або ж останньому символах пакета (на межі однойменних символів).

За результатами моделювання каналу зв'язку з використанням циклічного та монолітного кодів, наведеними в дисертаційній роботі [3], експериментально підтверджено переваги останнього щодо спрощених виявлення і виправлення помилок та швидкості робочих процедур під час кодування і декодування інформації. На відміну від циклічного коду монолітний код виявився ефективним засобом пересилання інформації каналами зв'язку за умови, коли ймовірність спотворення даних не перевищує p = 0.01.

Постановка задачі

Основним завданням статті є дослідження нових високоякісних методів синтезу кодів на основі комбінаторних конфігурацій та принципу поліморфізму.

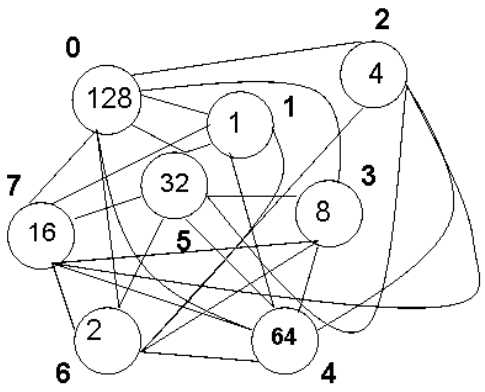
Побудова поліморфного коду

Під поліморфізмом розуміють здатність об'єкта змінювати свою структуру відносно поставлених або навколишніх умов. Метод полягає у тому, щоб будь-яке вхідне повідомлення володіло великою кількістю комбінацій, кодових послідовностей, а під час кодування одне і те саме значення кодувалося по-різному, змінюючи своє значення і довжину.

Секрет полягає у тому, щоб вхідне повідомлення (у нашому випадку це число, що характеризує букву у ASCII таблиці) подати як сукупність повідомлень, що характеризують складеність числа. Цей алгоритм подали на основі графу. Будь-який метод кодування можна подати у чотирьох найпоширеніших формах: це табличний, на основі кодового дерева або графу, геометричний та матричний метод представлення [4]. Тому для наочності алгоритм подамо на основі графу.

На рисунку подано повний граф, котрий складається з 8 вершин (кількість вершин може бути будь-яка). Кожна вершина графу містить значення (вагу), у нашому випадку для простоти та наочності взято числа степеня двійки. Значення ваг вершин графу розташовано хаотично. Кожна вершина графу має свій порядковий номер, котрий вибирають випадково.

Алгоритм полягає у тому, щоб розписати вхідне повідомлення як сукупність пакетів, що характеризують шлях проходження по вершинах графу, підсумовуючи або віднімаючи значення ваг вершин. Кінцем проходження шляху буде число, котре повинно дорівнювати числовому значенню вхідного повідомлення.



Повний граф, котрий складається з 8 вершин

Відносно формату пакета, в нашому випадку пакет може мати такий вигляд :

- номер наступної вершини графу (3 біти).
- знак дії (додавання, віднімання) над значення ваги наступної вершини, на котрий вказує перший елемент пакета (1 біт).
- ознака закінчення кодування повідомлення (1 біт).

Наприклад, закодуємо повідомлення, котре містить велику букву “А”, числовий аналог котрого дорівнює числу 65 (значення з ASCII таблиці). Розпишемо логічне проходження по графу як номер вершини та знак дії над значенням ваги вершини. Логічний запис для числа 65 матиме такий вигляд:

65 = **4+1**➔64+1;

65 = **0-1-4+6**➔128-1-64+2;

65 = **7+5+1+3**➔16+32+1+8,

де перший елемент – це номер вершини, вага якої – нам потрібне число, другий елемент – знак арифметичної дії над наступним значенням елементу, що записаний у логічній послідовності. У бінарному коді три варіанта коду числа 65 матимуть такий вигляд:

65 = (4+1)➔ 1001000111;

65 = (0-4+1)➔ 00000001001000001011;

65 = (7+5+1+3)➔ 11110101100011001111.

Як бачимо з прикладу, результуючі коди не подібні між собою, мають різну довжину та значення, але насправді вони означають те саме повідомлення.

Цей метод передбачає захист від злому, але не захищає інформації від помилок у фізичному каналі. Властивості завадостійкості код набуває після перетворення закодованої інформації на монолітний код.

Кільцевий монолітний код

Одним із шляхів підвищення якості даних є застосування надлишкового коду. Всі відомі надлишкові коди можна використати для виявлення помилок. Режим виправлення помилок здебільшого застосовують у тому випадку, якщо в каналі зв’язку є незалежні помилки або пакети помилок. Виправлення помилок часто приводить до невиправданих затрат обладнання на пристрої кодування і декодування. Одним з методів у комбінаторних конфігураціях є кільцевий монолітний код.

Особливості монолітного коду випливають зі способу формування дозволених комбінацій. Легко побачити, що будь-яка з таких комбінацій ланцюгового монолітного коду є помилковою, оскільки у всіх них зустрічаються символи “1” серед нулів (те саме можна сказати й про розміщення символів “0” серед одиниць): 1110001000,000111101, 1101010001. Якщо в монолітному коді з’являються хибні символи, то всі вони або частина з них зразу ж виявляються за вищезгаданою ознакою, що спрощує процедуру виявлення та виправлення помилок. Для усунення помилок достатньо хибні символи замінити істинними за правилом: “більшість однойменних символів повинні утворювати неперервну послідовність”. Одержаний результат випливає з вищезгаданої властивості монолітного коду: три перші комбінації виправляють за ознакою зв’язності однойменних символів: 111000000,000111111,11110000.

Властивість “зв’язаності” однойменних символів не дає змоги виправити помилки в комбінації 1101010001, оскільки це призводить до різних варіантів виправлення помилок: 1111000000,1111100000, 1111110000. Виявленню підлягають будь-які помилкові комбінації, але за умови, що хибні сигнали відсутні на місці розмежування різнойменних символів.

Використання надлишкових кодів для підвищення достовірності передавання інформації вимагає від проектувальника врахування різноманітних факторів, аналізуючи які, можна обрати код, дослідити розподіл помилок в каналі зв’язку, визначити допустиму ймовірність помилок кодової послідовності, досягти високої швидкості пересилання інформації, враховуючи складність алгоритмів пристроїв кодування і декодування, забезпечити необхідну надійність.

Відомо, що коригуючий код, побудований на основі ідеальної кільцевої в'язанки, має велику перевагу порівняно з класичними кодами завдяки спрощеним алгоритмам виявлення і виправлення як незалежних помилок, так і пакетів помилок.

Отже, вибір методу підвищення достовірності пересилання інформації залежить від багатьох факторів, серед яких основними є достовірність прийому, допустима швидкість пересилання даних вид помилок у каналі зв'язку.

Висновок

Використання запропонованого методу побудови коду є перспективним, оскільки не вимагає складних математичних дій для кодування та декодування, забезпечує надійність захисту інформації як від "чужих очей", так і від вад фізичного каналу. Для доступу до інформації потрібно знати такі характеристики:

- відносно монолітного коду:
  - значення розрядності монолітного коду;
  - комбінацію значень числового ряду;
  - розмір та формат пакетів закодованого монолітного коду;
- відносно поліморфного коду:
  - значення кількості вершин у графі;
  - числове знання та розташування ваг вершин у графі (для графу з 8 вершин комбінація розміщень ваг дорівнює 40320, а для 17 вершин $3*10^{15}$ комбінацій);
  - розмір та формат пакетів.

Щодо завадостійкості коду, експериментально підтверджено, що монолітний код забезпечує знаходження від 99,7 до 100 % помилок з числом розрядів більшим за 30, причому його висока захищеність зберігається зі збільшенням кратності помилок [5]. Зі збільшенням розрядності монолітного коду спостерігається експоненційна залежність зростання кількості виправлених помилок.

Однак при цьому спроможність виправлення багатократних помилок зменшується. Наприклад, у випадку однократних помилок з числом розрядів 33 виправляється в середньому 74,4 % помилок, тоді як двократних з числом розрядів 38–54.8 %, а п'ятикратних – лише 31,2 %. Отже, спроможність монолітного коду щодо виявлення помилок є набагато вищою від спроможності виправлення помилок.

У загальному випадку недоліком поліморфно-завадостійкого коду є його габаритність, оскільки поліморфна частина кодування істотно збільшує розмір закодованого повідомлення, при тому фізичний зміст коду стає настільки хаотичним, що архівувальні системи не дають практично жодного результату, але цю проблему вирішує монолітний код. Оскільки монолітний код складається в основному з пакетів нулів та одиниць, ця здатність дає велику перевагу у разі стисненої інформації.

1. Цимбал В.П. Теория информации и кодирование. – К.: Вища шк., 1982. – 304 с. 2. Різник В.В. Комбінаторні моделі і методи оптимізації в задачах інформатики: Навч. посібник. – К.: НМК ВО, 1991. – 72 с. 3. Кісь Я.П. Моделювання та синтез завадостійких кодів за допомогою ідеальних кільцевих в'язанок: Автореф. дис. …канд. техн. наук. – Львів, 1998. – Машинопис. 4. Журавський Ю.П., Полторак В.П. Теорія інформації та ковування. 5. Бандирська О.В., Велика О, Садов'як Б., Різник В. Дослідження кільцевого монолітного коду методом імітаційного моделювання // Вісн. Держ. ун-ту "Львівська політехніка". – 2003. – № 481. – С. 110–115.