УДК 519.725 **doi: 10.26906/SUNZ.2022.2.051**

Я. Є. Корсунська, І. В. Ільїна

Харківський національний університет радіоелектроніки, Харків, Україна

ДОСЛІДЖЕННЯ МЕТОДУ КОДУВАННЯ ТРАФІКА В ЗАХИЩЕНИХ КАНАЛАХ ПЕРЕДАЧІ ІНФОРМАЦІЇ

Анотація. Наш сучасний світ, наше сучасне суспільство можна цілком і повністю назвати інноваційною та інформаційною спільнотою, в якій технології розвиваються стрімко. Це стрімкий розвиток комунікацій та технологій дозволив вивести поняття "інформація" на новий рівень. Завдяки комп'ютерним технологіям людство навчилося передавати та обробляти інформацію у неймовірно великих обсягах. Оперативність обробки так само зробила крок вперед. Всі ці інновації дали величезний поштовх у розвитку розповсюдження інформаційних продуктів і послуг. Все це стало більш мобільним та модернізованим з появою, майже у кожного користувача, персонального електронного комп'ютерного обладнання та розширення телекомунікаційних систем. З кожним днем стала збільшуватись потреба у розробці та застосуванні ефективних рішень в інформаційних сферах. Збільшилася кількість виробництва апаратного та програмного забезпечення. Інформаційні технології для отримання та обробки нових знань також вимагали вдосконалення. З розвитком усіх нових технологій та інформацій, стало зароджуватися інформаційне суспільство в якому потрібно обробляти, захищати та передавати ті чи інші відомості через мережу. Ця стаття присвячена аналізу методів кодування трафіку, їх властивостей, відмінностей та вибору найбільш оптимального методу для захищених каналів передачі інформації.

Ключові слова: комп'ютеризовані системи та мережі, система захисту інформації, адаптивне кодування, широкосмугові сигнали, сигнально-кодові конструкції.

Вступ

Опис проблеми у загальному вигляді: модернізація апаратного та програмного забезпечення обробки, захисту та передачі всієї інформації в удосконалених комп'ютерних системах та мережах із стандартизованими методами захисту інформації, які виконують операцію адаптації та відповідають вимогам мінімальних апаратних та енергетичних витрат, є найбільш актуальним науково-практичним завданням у даному напрямі [1-6].

У сфері одноманітних засобів захисту існує потреба у створенні функціональних систем захисту. Їх основа лежить у методах адаптивного кодування, які застосовують зміни особливостей системи передачі за двома параметрами, що вимірюються: енергетичний виграш за сет кодування і швидкість передачі, щоб забезпечити найбільш сприятливе співвідношення виграшу до заданої швидкості при різноманітних станах інформаційного каналу. Під час процесу адаптивного кодування необхідно вирішити наступні основоположні завдання:

− визначити яку якість має інформаційний канал зв'язку;

− зробити висновок про зміну значень параметрів кодера та декодера, щоб забезпечити задану ймовірність доведення повідомлення, при мінімальній надмірності коду;

− встановити нові параметри коду в кодувальному та декодувальному пристрої.

Аналіз існуючих рішень

В даний час відомі деякі методи зміни параметрів коду за результатами повідомлення, а більш дієва двоконтурна схема корекції параметрів коду в залежності від якості каналу зв'язку по суті не використовується [7]. Методи визначення якості каналу зв'язку за результатами декодування коду та методи реалізації завадових кодів зі змінними параметрами мало вивчені. Основний прорив у здійсненні систем із зворотним зв'язком може бути показаний при використанні методів адаптивного кодування. Використання останніх дозволить створити основу розробки універсальних пристроїв захисту від помилок у складі уніфікованого ряду кінцевих пристроїв передачі даних. Це дасть поштовх, використовуючи єдиний пристрій захисту від помилок створити не тільки адаптацію до поточних змін статистики помилок каналу зв'язку, але і догодити широкому діапазону вимог до правдивості передачі інформації для різних видів зв'язку. Основними параметрами завадостійкого коду є [8]:

- блокова довжина (блокові коди) або довжина кодового межі (згорткові коди);

- швидкість коду, яка визначає його надмірність та коригуючу здатність.

Тим не менш, зміна параметрів коду лише часом гарантує необхідну мінімальну кодову відстань, і стійкість до перешкод може знижуватися. У зв'язку з тим, що алгоритми кодування і декодування певних кодів прив'язані до структури поліномів коду, що породжують і перевірочні, не всі завадостійкі коди можуть легко змінювати свої параметри. На даний момент є параметри коду, які можуть бути застосовані в якості параметричної адаптації. Слід зарахувати кількість інформаційних та надлишкових розрядів, що припадають на кодову комбінацію або список слів, що підлягають передачі. Існує безліч різних варіантів корекції параметрів коду, що ґрунтуються на видаленні або додаванні перевірочних, інформаційних символів (рис. 1). Перший варіант адаптивної корекції коду полягає у зменшенні інформаційних розрядів і називається укороченням коду [9]. Така процедура не призводить до підвищення швидкості коду.

$$R(i) = \frac{k-i}{n-i} \text{ коли } i = (0, f) \text{ та } n > k. \qquad (1)$$

Існує функція (1) монотонно спадаюча. Такий підхід у системах обміну інформацією ефективний для вирішення завдання зниження складності

кодуючих та декодуючих пристроїв, при виконанні умови досягнення необхідної виправляючої здатності коду. Іншим варіантом зміни параметрів коду є техніка перфорації або виколювання перевірочних розрядів. Перфорація лінійних блокових кодів полягає у видаленні перевірочних символів і це призводить до лінійного блокового коду з параметрами (n−f, k, d′), у якого мінімальна відстань d′ < d. Коли швидкість коду буде зростати, число перевірок зменшиться. Така технологія схожа на видалення певних стовпців з одиничної матриці перевірок.

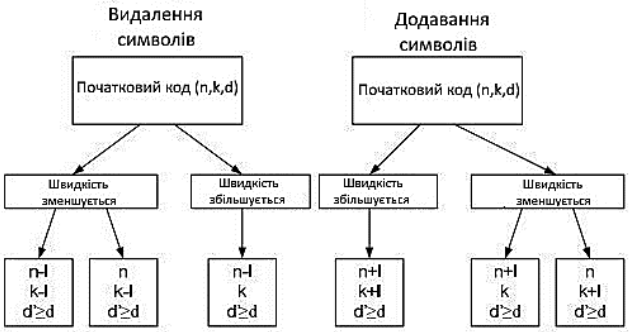

Рис. 1. Способи корекції параметрів завадових кодів

Є сумісні за швидкістю, перфоровані згорткові коди (rate compatible punctured convolution codes RCPC codes). Ці коди базуються з низько швидкісних кодів за допомогою періодичної перфорації, тому може бути збільшено швидкість коду. Якщо материнський код є згортковим кодом швидкості 1/2, тоді матриці перфорації P(1)-P(4) породжують RCPC коди зі швидкістю 4/5, 4/6, 4/7, 4/8 відповідно. В адаптивних системах з автоматичним перепитуванням RCPC коди знайшли своє використання, за допомогою їхньої здатності до нарощування надмірності, а також способу побудови кодів зі змінною швидкістю або кодів з нерівною захистом [10].

Застосовується ще один варіант розширення будь-якого двійкового (n, k, d) коду до коду зі значенням d_{min}= d + 1, за допомогою додатку до кожної кодової комбінації результату складення за модулем 2 її символів. Повторення таких кодових комбінацій створює підвищення мінімального відстані до двох. При цьому швидкість коду зменшується вдвічі. Подовження та поповнення коду полягає у підвищенні числа інформаційних символів, яке згодом тягне за собою збільшення розмірів матриці, що породжує. Як правило, такі коди з коригуванням параметрів, на приймальній стороні декодуються і за допомогою алгоритму спискового декодування, який забезпечує покращене співвідношення між складністю та ймовірністю помилки, ніж інші алгоритми. Для каналів з випадковим характером помилок практична увага передбачає лише кілька кодів з 10 популярних. Рідше автори користуються 3 види кодів: згорткові, Ріда-Соломона і турбо коди, до них відносяться коди з низькою щільністю випробування на парність (Low Density Parity Check codes - LDPC) [11].

Сукупність кількох схем завадостійкого кодування дозволяє брати до уваги різні обставини експлуатації. Наприклад згортковий код зазвичай застосовується передачі мовного трафіку, коли можливість помилки на біт, може бути досить великий , але некритичної сприйняття і усвідомлення переданої інформації. При передачі даних використовуються, наприклад, іменовані каскадні коди, яких зовнішнім зазвичай вважається код Ріда-Соломона, а внутрішній згортковий.

Для зведення адаптивних систем кодування між завадовими кодами велику увагу приділяють сумісним за швидкістю, перфорованим згортковим кодам (Rate Compatible Punctured Convolutional Codes – RCPC) та гніздовим (вкладеним) згортковим кодам (Nested Convolution Codes – NCC). Гніздові згорткові коди є комплектом кодів зі швидкістю R = 1/(n+1), які вважаються похідними від згорткового коду швидкості R = 1/(n+1), за допомогою пошуку найкращих генераторних послідовностей Gn+1(D). Таким чином, застосовуючи технологію розкладання материнського згорткового коду на систему гніздових (вкладених) згорткових кодів, можливо отримати об'ємний комплект кодових відповідностей (ЕВК), при цьому зберігаючи структуру та метод кодування материнського кодека На даний час синтез гніздових згорткових кодів, а також їх якості досліджуються, попре ще залишається незакритим питання про декодування гніздових згорткових кодів. Втім надається увага будівництву адаптивної системи кодування на базі RCPC та NCC кодах, яка допускає зміни по 2 вимірам: отримання необхідної величини виграшу за рахунок кодування та забезпечення різних вимог до інформаційної та канальної швидкості.

Сигнально-кодові системи для систем широкосмугового доступу

Усі сигнально-кодові системи відповідно до активної задачі, яка вирішується, поділяються на групи. При створенні нового покоління СКС (сигнально-кодових систем) одним з вимог вважається уніфікація за застосовуваними видами модуляції в частині ширини діапазону радіовипромінювання. Детальне опрацювання вимог до прогресивних систем радіозв'язку дозволила утворити 4 основні групи сигнально-кодових систем.

1. СКС, що застосовуються для автоматичного встановлення та ведення з'єднання. Характеризуються високою стабільністю до шумових, структурних, імпульсних і вузькосмугових перешкод, а також багатопроменевому поширенню, допплерівському розмиттю та зміни частот у каналі. Ця група базується на шумоподібному сигналі, створюваному як розділений код із граничною відстанню.

2. Сигнально-кодові системи, що застосовуються для середньо швидкісної передачі даних. За рахунок надвеликого канального алфавіту сигнально-кодової системи, 224 і більше канальних знаків, що розрізняються, швидкість передачі 2400 біт/с гарантується при тривалості канального знаку 20 мс, Це все дозволяє працювати за умов міцної багатопроміневості. Створені трансформації ще забезпечують роботу за умов вузько смугових та імпульсних перешкод у смузі сигналу [12].

3. СКК швидкісної (більше 2400 біт/с) передачі даних. В даний час ведуться роботи з нового

покоління даних сигналів, які володіють більш невисоким пікфактором в порівнянні з сигналами паралельних (OFDM) модемів. Сигнали не стануть потребувати накладних процедур коригування імпульсної властивості каналу, що займають у модемах послідовного типу за стандартом MIL-STD-188-110B до 25% пропускної спроможності каналу.

4. СКК на кшталт CHESS (Correlated Hopping Enhanced) Спред Spectrum), що використовують розширення діапазону сигналу корельованими стрибками за частотою. Дана група сигналів зумовлена передачою невеликих обсягів інформації. При швидкості псевдовипадкової перебудови за частотою до 200 стрибків за секунду в смузі до 10 мгц, сигнали цього типу мають високу скритність і характеризуються стабільністю. Це працює з виявленням, перехопленням натуральних та штучного походження перешкод [13]. Співвідношення енергетичної продуктивності від притаманної швидкості для різних систем широкосмугового доступу представлено на рис. 2, де пов'язано перешкодостійкість із пропускною можливістю.

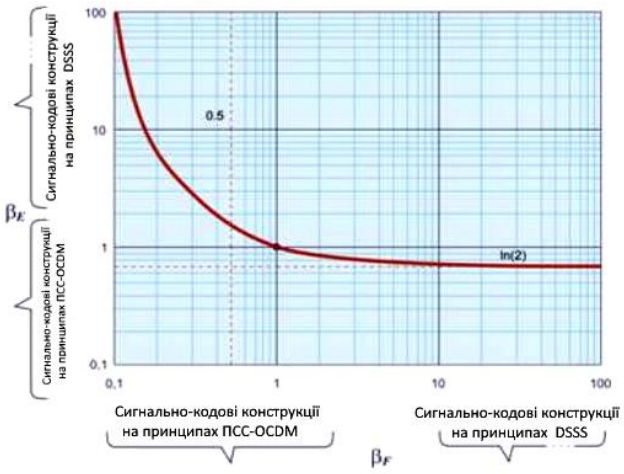

Рис. 2. Залежність енергетичної ефективності від питомої швидкості

З графіка випливає, що залежно від мети застосування системи зв'язку, можна позначити 3 провідних напрями зведення сигнально-кодових систем [14]:

− сигнально-кодові системи на базі OFDM сигналів для систем зв'язку, що забезпечують найбільшу пропускну здатність для даних смуг пропускання та можливості промахів в умовах натуральних перешкод;

− сигнально-кодові системи на базі CDM сигналів з прямим розширенням діапазону (DSSS) для систем зв'язку з найбільшою стійкістю до перешкод по критеріях впливу кожних перешкод;

− сигнально-кодові системи для систем зв'язку з максимально ймовірними перешкодостійкістю та пропускною можливістю в критеріях внутрішньо-системних та зовнішніх перешкод, які отримали назву ортогонально-кодовий розподіл каналів (OCDM).

Важливим дефектом при застосуванні цих типів СКС у спільній смузі частот вважається спектральне вторгнення сигналів, що тягне за собою нарощування характерних витрат смуги пропускання. Перешкодозахищеність 3-х розглянутих технологій створення систем широкосмугового доступу може бути значуще підвищена методом реалізації сигнально-кодових систем, на базі сигналів зі штучно створюваним широкосмуговим діапазоном.

Оцінка якості каналу зв'язку в системах передачі інформації

Одним із способів контролю каналів передачі даних вважається контроль за вторинними статистичними рисами – статистиці помилок в черговості дискретних складових та блоках інформації з урахуванням залежного від сутності їх заломлення. Для оцінки змінної ймовірності застосовується, як правило, коефіцієнт помилок по одиночним складовим (кодовим комбінаціям). Втім, його використання цілеспрямовано тільки на канали з розподілом помилок, найближчим до незалежного. Оцінка стану каналів, характеризуються групуванням промахів складових (що призводить до зв'язку спотворень блоків інформації). При застосуванні вказаного способу стає очевидно неприйнятним і веде до великих помилок контролю. Внаслідок цього застосовність цього методу обмежується часом квазістаціонарності стану каналу зв'язку.

Популярним є метод контролю якості каналу зв'язку, при якому на виході каналу із прийнятої випробувальної послідовності віднімають передану випробувальну послідовність, і в результаті отримують послідовність помилок, а потім обчислюють характеристики каналу зв'язку, що характеризують його якість. Дефектом даного методу вважається зниження швидкості передачі необхідної інформації, яке обумовлене тим, що визначення якості каналу зв'язку роблять під час передачі каналом випробувальної послідовності, і канал у це час використовується для вимірювань. Контроль якості каналу зв'язку приймається приймальною стороною за підсумками декодування текстів внутрішнього завадостійкого каскадного коду. При цьому характеристики каналу зв'язку описують двома параметрами: середньою можливістю промахів на біт та коефіцієнтом групування помилок за змінною моделі каналу зв'язку Пуртова.

Дефектом цього методу вважається невисока достовірність контролю, тому що у каналах невисокого якості отримання неспотвореного способу текстів перешкодостійкого коду може відбуватися з невеликою можливістю. Ще достовірність контролю знижується через те, що на прийомній стороні незрозуміло чисельність переданих текстів завадостійкого коду.

При аналітичному дослідженні чи статистичному випробуванні дискретних каналів дуже широко використовуються ймовірнісні характеристики потоку помилок на виході інформаційного каналу.

Зазвичай такі характеристики використовуються:

− усереднена ймовірність появи помилки на безлічі вихідних символів ДКС;

− ймовірність спотворення кодової послідовності P(i(1,n)) на безлічі кодових послідовностей на виході інформаційного каналу;

− функція кратності помилок P(m,n), яка визначається як ймовірність появи m помилок на кодовій послідовності довжини n.

Знання цих характеристик, з одного боку, дозволяє визначити властивості реальних каналів зв'язку та розробити на їх основі математичні (імітаційні) моделі, алгоритми яких описують з достатнім ступенем точності.

З іншого боку, ці характеристики дають можливість оцінити ймовірність помилкового декодування при використанні кодів із заданою кодовою відстанню в режимі виправлення помилок за мінімальною Хемінговою відстанню, не проводячи складних процедур кодування та декодування.

Висновки

У комплексі завдань розробки та створення єдиної автоматичної системи управління вагомий простір належить реалізації високоефективних уніфікованих апаратно-програмних модулів захисту та передачі інформації.

Зростання запитів до достовірності та своєчасності передачі інформації в призначених комп'ютерних системах у поєднанні з вимогами до імовірнісно-часових рис доведення повідомлення потребує поліпшення та розробки універсальних засобів захисту та передачі інформації. Зроблений аналіз в області проектування апаратно-програмного забезпечення для передачі інформації в комп'ютеризованих вбудованих системах показав, що немає єдиного методологічного підходу, спрямованого на створення універсальних модулів захисту інформації, яке дозволяло б гарантувати належну відповідність енергетичного виграшу та швидкості передачі. Головним дефектом інформаційних систем передачі даних в автоматичних системах зв'язку – кожний прилад захисту від помилок розробляється під кожний образ каналу зв'язку, що породжує велику кількість різних пристроїв, які реалізують ту саму функцію – захист інформації від помилки. Існуючі методи захисту інформації від помилок не передбачають топологію потоку помилок на виході справжніх каналів зв'язку. Таким чином, метою цієї статті вважається розгляд засобів збільшення достовірності та швидкості передачі інформаційних повідомлень у комп'ютеризованих вбудованих системах, на базі розробки та покращення уніфікованих способів та алгоритмів захисту та передачі інформації, що реалізуються на прогресивній елементної основи.

СПИСОК ЛІТЕРАТУРИ

1. Sojuyigbe S., Daniel K. Wearables/IOT devices: Challenges and solutions to integration of miniature antennas in close proximity to the human body. Electromagnetic Compatibility and Signal Integrity, 2015 IEEE Symposium, March 2015.
2. Gagliardone I., Gal, D., Alves, T. and Martinez, G.: Countering Online Hate Speech. UNESCO, Paris, France, 2015.
3. Мірошник М.А. Методи захисту цифрової інформації у розподілених комп'ютерних мережах/М.А. Мірошник // Інформаційно – керуючі системи на залізничному транспорті – 2014. – №5, с.66-70.
4. Рентюк В. Короткий путівник бездротових технологій «Інтернету речей». Частина 1. Мережі, шлюзи, хмари та протоколи // Control Engineering Росія. 2017. №6.
5. Рентюк В. Короткий путівник бездротових технологій «Інтернету речей». Частина 2. Близький радіус дії// Control Engineering Росія. 2018. №1.
6. Рентюк В. Короткий путівник бездротових технологій «Інтернету речей». Частина 3. Wi-Fi// Control Engineering Росія. 2018. №2.
7. Рентюк В. Короткий путівник бездротових технологій «Інтернету речей». Частина 4. Великий радіус дії// Control Engineering Росія. 2018. №3.
8. Рентюк В. Електромагнітна стійкість: проблема, рішення якої не йдуть // Компоненти та технології. 2017. №7.
9. Збільште термін служби батареї мобільного або бездротового пристрою (5991-0519EN).
10. Крилова В.А. Реалізація адаптивного пристрою кодування/декодування на ПЛІС / В.А. Крилова // Вісник НТУ "ХПІ". - Харків: НТУ «ХПІ», 2014. − №15 (1058) – С. 86-90.
11. Галушкін, А.І. Нейронні мережі: історія розвитку теорії: Навчальний посібник для вузів. / А.І. Галушкін, Я.З. Ципкін. - М: Альянс, 2015. - 840 с.
12. Каллан, Р. Нейронні мережі: Короткий довідник/Р. Каллан. - М: Вільямс І.Д., 2017. - 288 с.
13. Хайкін, С. Нейронні мережі: повний курс / С. Хайкін. – М.: Діалектика, 2019. – 1104 с.
14. Ширяєв, В.І. Фінансові ринки: Нейронні мережі, хаос та нелінійна динаміка / В.І. Ширяєв. - М: Ленанд, 2019. - 232 с

Received (Надійшла) 30.03.2022
Accepted for publication (Прийнята до друку) 11.05.2022

Study of the traffic encoding method in secure information transmission channels

Y. Korsunskaya, I. Ilina

Abstract. In the era of global informatization, social networks are of great importance for obtaining various information by network users. But it must be taken into account that social networks such as Facebook, Twitter, instagram contain billions of raw unstructured data, the processing of which is indeed quite a difficult task to study. Data mining allows you to extract current information from a large number of data sets, structure and, after the analysis, gain knowledge by detecting patterns between data, which makes it possible to predict changes in the network that have occurred based on the interactions of information flows and events. This information is used in various fields such as business, education, medicine, cyber security, etc. The field of data mining has made huge strides from its inception to its current level, but Data Mining continues to face many challenges, especially when processing social media data. This article is devoted to the analysis of various data mining methods that are used for social network analysis, as well as the study of the most priority areas in the field of data mining based on the review of various studies, and also focuses on the field of data mining in social networks, which will be used in further research.

Keywords: computerized systems and networks, information security system, adaptive coding, broadband signals; signal-code structures.