УДК 004.934 DOI: 10.31673/2412-4338.2020.010411

Коляда К. В., Марковський О. П., Саверченко В. Г. *Національний технічний університет України «Київський політехнічний інститут імені Ігора Сікорського», Київ, Україна*

Торошанко А. І. *Сумський державний університет, Суми, Україна*

МЕТОД РЕЗЕРВУВАННЯ ТА ВІДНОВЛЕННЯ ВТРАЧЕНИХ ДАНИХ В ГЛОБАЛЬНИХ МЕРЕЖАХ

Запропоновано метод формування резервних пакетів при передачі даних в глобальних мережах, а також технологія їх використання для відновлення втрачених чи пошкоджених пакетів. Розглянутий метод гарантованого відновлення не більше трьох втрачених чи пошкоджених пакетів. Наведено математичне та технічне обґрунтування запропонованого методу. Кожен з надлишкових резервних пакетів пропонується формувати у вигляді логічної суми певних підмножин інформаційних пакетів. Математично доведено, що викладені правила формування контрольних пакетів забезпечують існування ортогональної системи рівнянь, вирішення яких визначає процес відновлення втрачених інформаційних пакетів. На основі отриманих теоретичних результатів розроблено технологію формування резервних пакетів, які передаються разом з інформаційними пакетами..

Для прискорення відновлення втрачених пакетів метод передбачає використання спеціальних таблиць передобчислень. Детально викладена технологія формування таких таблиць які містять специфікації відновлення втрачених пакетів для різних варіантів втрат пакетів (інформаційних чи резервних). Кожен втрачений пакет відновлюється у вигляді логічної суми визначених специфікацією множин невтрачених інформаційних чи резервних пакетів. Розроблений спосіб формування специфікацій забезпечує низьку обчислювальну складність процесу відновлення пакетів.

Основна перевага запропонованого методу відновлення втрачених пакетів в глобальних мережах, в порівнянні з відомими, полягає в прискоренні процесу реконструкції втрачених пакетів за рахунок використання простих лінійних перетворень. Це відкриває можливості відновлення втрачених інформаційних пакетів в глобальних мережах в реальному часі. Запропонований метод забезпечує високу ефективність апаратної реалізації.

***Ключові слова**: глобальна мережа, надійність передачі даних, відновлюючі коди, відновлення втрачених пакетів, лінійні коди, реконструюючі коди, передобчислення.*

Koliada K. V., Markovskyi O. P., Saverchenko V. G. *National Technical University of Ukraine "Igor Sykorsky Kiev Polytechnic Institute", Kyiv, Ukraine*

Toroshanko A. I. *Sumy State University, Sumy, Ukraine*

METHOD OF REDUNDANCY AND LOSS DATA RECOVERING IN GLOBAL NETWORKS

A new method of redundant packet formation for data transmission in global networks, as well as a technology of their usage for restoring of lost and damaged data packets is proposed. The method for guaranteed restoring not more then three lost and damaged data packets is presented. Mathematical and technical justification of the proposed method is given. Each of the redundant reserve packet proposed to form as the logical sum of certain subsets of data packets. Formed reserve packets are transmitted together with information packets. The rules of redundancy packets formed whose ensures of the existence of an orthogonal system of equations, which solves the process of reconstruction of lost information packets are mathematically rigorously proven. Based on obtained theoretical results the technologies for redundant packet formation for data transmission in global networks has been developed.

To accelerate the reconstruction of lost packets, the method involves the usage of special pre-computational tables. The technology of forming such tables whose contained specifications for lost packets restoring for different variants packets (main or redundancy) loss is described in detail. Each reconstructed packet is restoring as the logical sum of predefined by specification subsets of data and redundant reserve no loss packets. The developed method for specification forming ensured the low calculation complexity of packets restoring process.

The main advantage of the proposed method for restoring of lost data packets in global networks in comparison with known methods consist of accelerating of packets reconstruction process by using simple transformation. This provides the possibility of reconstruction lost data packet in global networks in real time. The proposed method ensured high efficiency for hardware implementations.

Keywords: *global network, data security, recovery codes, recovery of lost packages, line codes, reconstruction codes, pre-computation.*

Коляда К. В., Марковский А. П., Саверченко В. Г. *Национальный технический университет Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина*
Торошанко А. И. *Сумской государственный университет, Сумы, Украина*

МЕТОД РЕЗЕРВИРОВАНИЯ И ВОССТАНОВЛЕНИЯ УТРАЧЕННЫХ ДАННЫХ В ГЛОБАЛЬНЫХ СЕТЯХ

Предложен метод формирования резервных пакетов при передаче данных в глобальных сетях, а также технология их использования для восстановления утраченных или поврежденных пакетов. Рассмотрен метод гарантированного восстановления не более трех потерянных или поврежденных пакетов. Приведены математическое и техническое обоснование предложенного метода. Каждый из избыточных резервных пакетов предлагается формировать в виде логической суммы определенных подмножеств информационных пакетов. Математически строго доказано, что изложены правила формирования контрольных пакетов обеспечивают существование ортогональной системы уравнений, решение которых определяет процесс восстановления утраченных информационных пакетов. На основе полученных теоретических результатов разработана технология формирования резервных пакетов, передаваемых по сети вместе с информационными пакетами.

Для ускорения восстановления потерянных пакетов метод предполагает использование специальных таблиц предвычислений. Подробно изложена технология формирования таких таблиц содержащие спецификации восстановления потерянных пакетов для различных вариантов потерь пакетов (информационных или резервных). Каждый потерянный пакет восстанавливается в виде логической суммы определенных спецификацией множеств неутраченных информационных или резервных пакетов. Разработанный способ формирования спецификаций обеспечивает низкую вычислительную сложность процесса восстановления пакетов.

Основное преимущество предложенного метода восстановления потерянных пакетов в глобальных сетях, по сравнению с известными, заключается в ускорении процесса реконструкции потерянных пакетов за счет использования простых линейных преобразований. Это открывает возможности восстановления утраченных информационных пакетов в глобальных сетях в реальном времени. Предложенный метод обеспечивает высокую эффективность аппаратной реализации.

Ключевые слова*: глобальная сеть, надежность передачи данных, восстанавливающие коды, восстановление потерянных пакетов, линейные коды, реконструирующие коды, предвычисления.*

1. Вступна частина

Постановка задачі. Швидкий прогрес технології глобальних мереж спричиняє динамічне розширення її застосування: Інтернет витісняє традиційні технології: телебачення та телефонію, а з появою портативних радіомодемів він активно використовується в системах дистанційного моніторингу стану об’єктів реального світу та управління ними в реальному часі. Це суттєвим чином підвищує рівень вимог до оперативності та надійності доставки даних в глобальних мережах [1].

В таких мережах транспортування пакетів даних здійснюється за різними маршрутами. При цьому існує можливість їх затримок внаслідок щільного трафіку, втрат при використанні peer-to-peer мережних технологій [2] або виникнення помилок передачі в ефірних каналах. Все це, з огляду на специфіку нових сфер застосування Інтернету, диктує необхідність застосування спеціальних засобів забезпечення оперативності та надійності доставки пакетів даних. Один з напрямків вирішення цієї нагальної проблеми полягає в

формуванні та передачі резервних пакетів, які можуть бути використані для швидкого відновлення втрачених чи затриманих понад критичний час інформаційних пакетів.

Таким чином, наукова задача підвищення ефективності резервування та відновлення даних в глобальних мережах є актуальною для сучасного етапу розвитку інформаційних технологій.

Аналіз літературних джерел. Динамічний прогрес засобів передачі інформації та мережевих технологій визначає швидкий розвиток засобів виявлення, локалізації та виправлення помилок передачі даних. Основна особливість задачі нейтралізації помилок передачі в глобальних мережах полягає в багаторівневому характері її вирішення[3]: як правило, виявлення помилок здійснюється на внутрішньопакетному рівні, на цьому ж рівні при обмеженій кратності помилок може здійснюватися їх локалізація [2] та виправлення. При більшій кратності помилок, які не можуть бути виправлені на внутрішньопакетному рівні, здійснюється повторна передача пакету [4], що суттєво збільшує час доставки інформації. Тому в сучасних глобальних мережах активно використовується виправлення помилок передачі даних на рівні пакетів [5], тобто коригуються не окремі біти чи символи пакету, а відновлюється весь пакет [6]. Використання такого підходу дозволяє також вирішувати задачі відновлення втрачених або затриманих понад встановлений часовий ліміт пакетів.

Використання класичних коригуючи кодів [7], які орієнтовані на комплексне вирішення задачі локалізації та виправлення помилок, на рівні пакетів неефективне в силу того, що задачу локалізації помилок непотрібно вирішувати.

До теперішнього часу запропоновано ряд способів [8-10] формування резервних пакетів і відновлення за їх допомогою втрачених інформаційних пакетів. В більшості робіт ця задача вирішується з позицій використання мінімальної кількості резервних пакетів. Відповідно, для цього використовуються нелінійні, зокрема, циклічні коди [8, 9]. Проте використання таких відновлюючих кодів потребує значних обчислювальних ресурсів для відновлення втрачених пакетів, об'єм яких експоненційно зростає з кількістю втрачених інформаційних пакетів. Фактично, для відновлення пакетів в тій чи іншій формі потрібно розв'язувати систему рівнянь. При використанні нелінійних відновлюючих кодів, відповідно, потрібно розв'язувати нелінійну систему рівнянь, що може бути виконане лише методом перебору. Це прийнятне лише при невеликій розмірності системи, зокрема не більшій 2-х [9]. Тому відомі методи втрачають свою ефективність при необхідності відновлювання трьох і більше втрачених пакетів. Крім того, використання нелінійних перетворень вимагає громіздких обчислень, апаратна реалізація яких потребує складних схем.

В роботі [10] для вирішення цих проблем пропонується використовувати лінійні перетворення, що дозволяє значно прискорити обчислювальну реалізацію процесу відновлення втрачених пакетів, а також спростити схему при апаратній реалізації. Проте запропонована в [10] схема дозволяє відновлювати лише частину втрачених пакетів. Тобто в цій схемі існують варіанти втрати резервних та основних пакетів, які не можуть бути відновлені. Іншими словами, схема [10] реалізує ймовірнісне відновлення втрачених пакетів.

Невирішені питання. На основі проведеного огляду та аналізу літературних джерел можна зробити наступні висновки. Створені до теперішнього часу методи реконструювання втрачених інформаційних пакетів з використанням резервних не забезпечують прийнятної для широкого кола практичних застосувань швидкості обчислювальної реалізації, що не дозволяє реалізувати відновлення втраченої інформації в реальному часі.

Основним резервом прискорення швидкості відновлення втрачених пакетів є використання простих в реалізації лінійних булевих перетворень спільно з оптимізаційним вибором багатоваріантних процедур реконструювання.

Мета та задачі дослідження. Мета досліджень полягає в прискоренні обчислювальних процедур формування резервних пакетів і відновлення гарантованої кількості інформаційних пакетів за рахунок використання лінійних логічних кодів, що

додатково забезпечує ефективну реалізацію апаратними засобами, а також оптимізації процедури реконструкції шляхом мінімізації кількості операцій.

Для досягнення поставленої мети в роботі розв'язуються такі наукові задачі:

– теоретичне дослідження властивостей надлишкових пакетів, які гарантують можливість відновлення інформаційних пакетів в разі втрати не більше трьох пакетів з їх загального числа;

– на основі отриманих теоретичних результатів розробка способу формування резервних пакетів для гарантованого відновлення інформаційних пакетів при втраті не більше трьох з загальної кількості пакетів, що передаються;

– розробка табличного способу відновлення втрачених інформаційних пакетів;

– розробка технології оптимізації процедури відновлення втрачених пакетів за критерієм мінімуму потрібних для цього операцій;

– оцінка параметрів технічної реалізації методу резервування та відновлення втрачених пакетів для аналізу ефективності в порівнянні з існуючими методами.

2. Теоретичне обґрунтування методу гарантованого відновлення втрачених інформаційних пакетів з використанням лінійних кодів

Для досягнення поставленої мети пропонується метод формування резервних пакетів та відновлення з їх використанням втрачених, пошкоджених або затриманих понад критичний час основних пакетів даних.

Пропонований метод базується на наступній моделі передачі пакетів в мережі. Інформація, яка передається організована у вигляді n основних пакетів $P_1, P_2, \ldots, P_n$. Пакети містять контрольні коди, які дозволяють виявити помилку, що виникла в процесі передачі.

Вважається, що передача пакетів здійснюється за різними маршрутами, в залежності від зміни трафіку. При цьому, маршрут передачі може включати фрагменти однорангових peer-to-peer мереж. Для таких фрагментів існує можливість некерованого відключення одного з них з тимчасовим порушенням віртуального каналу. При цьому може відбуватися втрата деяких пакетів.

Крім того, часто специфіка широкого кола практичних задач визначає критичний час доставки пакетів, після чого вони втрачають актуальність.

Таким чином, поняття втрати пакету включає три ситуації:

– виникнення помилок передачі, що не можу бути виправлені за допомогою вбудованих в пакет контрольних кодів;

– втрата пакету в процесі передачі;

– доставка пакету після визначеної граничної часової межі.

Для відновлення втрачених пакетів пропонується разом з n основними передавати k резервних пакетів $Q_1, Q_2, \ldots, Q_k$, які формуються спеціальним чином з інформації, що міститься в основних пакетах.

Задля швидкого відновлення втрачених основних пакетів пропонується формувати резервні пакети та відновлювати втрачені з використанням лінійних булевих перетворень. Важлива перевага застосування перетворень цього класу полягає в граничній простоті апаратної реалізації. Відповідно, кожен резервний пакет формується як сума за модулем два кодів певної підмножини основних пакетів:

$$\forall l \in \{1,2,...,k\} : Q_j = \bigoplus_{i=1}^{n} a_{l,i} \cdot P_l. \qquad (1)$$

де $\forall i \in \{0,\ldots,k\}$, $l \in \{1,2,\ldots,n\}$: $a_{i,l} \in \{0,1\}$.

Бінарні коефіцієнти a в формулі (1) утворюють матрицю **A**:

$$\mathbf{A} = \begin{vmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{vmatrix} = \begin{vmatrix} a_{1,1}\ a_{1,2} \cdots a_{1,n} \\ a_{2,1}\ a_{2,2} \cdots a_{2,k} \\ \vdots \\ a_{k,1}\ a_{k,2} \cdots a_{k,n} \end{vmatrix}.$$

На стороні приймача, в разі неотримання певної множини Ω основних пакетів до критичного моменту часу, вони вважаються втраченими і можуть бути відновлені шляхом виконання лінійних перетворень над отриманими вчасно основними і резервними пакетами.

При втраті трьох з $n+k$ пакетів можливо три ситуації:

1. Всі три втрачених пакети відносяться до основних.
2. Два втрачених пакета відносяться до основних і один із втрачених – резервний.
3. Один втрачений пакет відноситься до основних і два – до резервних.
4. Всі три втрачених пакети відносяться до резервних.

В останньому випадку всі основні пакети отримані на стороні приймача без помилок і вчасно – відповідно задача відновлення даних не вирішується.

Якщо втрачено два резервних пакета і один з основних, то задача полягає в відновленні саме одного основного пакету. Ця задача може бути вирішена, якщо після видалення з матриці **A** рядків, які співвідносяться з втраченими резервними пакетами, вона не буде містити нульових стовбців. Для цього достатньо, щоб всі стовбці матриці **A** містили більше двох одиниць, тобто виконувалася умова:

$$\forall l \in \{1,2,...,n\} : \sum_{i=1}^{k} a_{i,l} > 2\,. \tag{2}$$

Якщо втрачено два основних пакети і один з втрачених стовбців належить до резервних, то для відновлення втрачених основних пакетів необхідно, щоб після видалення з матриці **A** рядка, який співвідноситься з втраченим резервним пакетом, всі стовбці в ній були різними.

Для того, щоб ця умова виконувалася, Хемінгова відстань між стовпцями матриці **A** має бути більше одиниці:

$$\forall l, i \in \{1,2,...,n\}, l \neq i : \sum_{j=1}^{k} (a_{j,l} \oplus a_{j,i}) > 1. \tag{3}$$

Якщо всі три втрачені пакети відносяться до класу основних і виконуються умови (2) і (3), то втрачені пакети можуть бути гарантовано відновлені за умови, що матриця **A** містить рядок, який складається повністю з одиниць:

$$\exists j \in \{1,2,...,k\} : \prod_{i=1}^{n} a_{j,i} = 1\,. \tag{4}$$

Це може бути доведене наступним чином. Номери втрачених пакетів можуть бути позначені як v, w та e, v, w, $e \in \{1, 2, \ldots, n\}$, причому, не порушуючи загальності, можна вважати, що $v<w<e$.

Тоді можна розглядати матрицю **Δ**, утворену стовпцями v, w та e матриці **A**:

$$\Delta = \begin{vmatrix} a_{1,v}\ a_{1,w}\ a_{1,e} \\ a_{2,v}\ a_{2,w}\ a_{2,e} \\ \cdots \\ a_{k,v}\ a_{k,w}\ a_{k,e} \end{vmatrix}$$

Втрачені пакеті можуть бути відновлені, якщо в матриці **Δ** існують три рядки, які утворюють ортогональну матрицю **Θ**.

Для доведення цього факту доцільно дослідити диференційні властивості рядків матриці **Δ**. Ці властивості для кожного y-го рядка матриці **Δ**, $y \in \{1, 2, \ldots, k\}$

характеризуються двокомпонентним бінарним вектором $d_y = < d_{y1}, d_{y2} >$ який визначається наступним чином:

$$d_y = <d_{y1}, d_{y2}>, \quad \text{де } d_{y1} = a_{y,v} \oplus a_{y,w},\ d_{y2} = a_{y,v} \oplus a_{y,e}.$$

Згідно з (3) Хемінгова відстань між першим та другим стовпчиками матриці Δ не менше 2-х. Це означає, що в матриці в матриці Δ існує не менше двох рядків, для яких перша компонента вектору d дорівнює одиниці, тобто d =<1, 0> або d=<1, 1>. При цьому, в силу того, що кожному значенню вектору d співвідносяться два можливих рядки матриці Δ може бути дві ситуації: два рядки, в яких відрізняються значення першого та другого стовпчиків є інверсією одне одного, тобто співвідносяться одному значенню d (наприклад, рядки 101 та 010 є інверсними і співвідносяться значенню d =<1, 0>) або зазначені рядки співвідносяться різним значенням d і, відповідно, не є інверсними (наприклад рядок 101, що співвідноситься з d =<1, 0> та рядок 011, що співвідноситься з d=<1, 1>). Оскільки кожному значенню вектору d співвідносяться два можливих рядки матриці Δ, то, відповідно, існує не менше двох рядків матриці Δ, які належать множині: $\mathbf{Y_1}$ = { <0, 1, 0>, <1, 0, 1>, <0, 1, 1>, <1, 0, 0>}.

Цілком аналогічно можна зробити висновок про те, що в матриці Δ точно є не менше двох рядків в яких відрізняються перший та третій стовпчики, а значить, друга компонента вектору d дорівнює одиниці: d = <0, 1> або d=<1, 1>. Рядки, з відмінними значеннями першої та третьої компоненти можуть співвідноситися або з одним із зазначених значень d, або з різними. Відповідно, це означає, що в матриці Δ є не менше двох рядків, які належать множині $\mathbf{Y_2}$ = {<0, 0, 1>, <1, 1, 0>, <0, 1, 1>, <1, 0, 0>}.

За аналогією правомірно стверджувати, що в матриці Δ існує не менше двох рядків, в яких відрізняються другий та третій стовпчики, тобто для яких d=<0, 1> або d=<1, 0>. Вказані рядки можуть бути інверсними, тобто співвідноситися з одним із зазначених значень d, або не інверсними, що означає їх відповідність обом із значень d.

З вищевказаного випливає факт наявності в матриці Δ не менше двох рядків, які належать множині $\mathbf{Y_3}$ = {<0, 0, 1>, <1, 0, 1>, <0, 1, 0>, <1, 1, 0>}.

Очевидно, що перетин кожної пари множин $\mathbf{Y_1}$, $\mathbf{Y_2}$, $\mathbf{Y_3}$ містить рівно дві компоненти, проте перетинів всіх трьох множин – жодних, тобто $\mathbf{Y_1} \cap \mathbf{Y_2} \cap \mathbf{Y_3} = \varnothing$. Для того, щоб виконувалася умова (3) потрібно, щоб в матриці Δ існували два рядки які належать $\mathbf{Y_1}$, два рядки, що належать $\mathbf{Y_2}$ та два рядки, які належать множині $\mathbf{Y_3}$.

Якщо два наявні в матриці Δ рядки, що належать множині $\mathbf{Y_1}$ не є інверсними, то вони співвідносяться з двома різними значеннями d. У випадку, коли вказані два рядки інверсні по відношенню один до одного і співвідносяться з одним значенням d_1, то вони належать також до множин $\mathbf{Y_2}$ або $\mathbf{Y_3}$. Якщо вони належать $\mathbf{Y_1}$ і $\mathbf{Y_2}$, то для виконання (3) має існувати ще пара рядків, які належать $\mathbf{Y_3}$ і співвідносяться з $d_2 \neq d_1$. Аналогічна ситуація має місце і коли пара рядків одночасно належать множинам $\mathbf{Y_1}$ і $\mathbf{Y_3}$.

З наведеного випливає, що для виконання умови (3) в матриці Δ мають існувати рядки, які співвідносяться до мінімум двох різних значень d.

В таблиці 1 наведені всі можливі варіанти значень пари рядків матриці Δ, які співвідносяться з двома різними значеннями d. В таблиці 1 ці пари рядків доповнені рядом, яких складається з самих одиниць і який існує в матриці Δ згідно (4).

Таблиця 1

Ортогональні підматриці матриці Δ при всіх можливих парах значень d

Можливі пари векторів d	Можливі набори рядків, що співвідносяться парі значень d з одичним рядом			
<0, 1> , <1, 0>	0 0 1 0 1 0 1 1 1	0 0 1 1 0 1 1 1 1	1 1 0 0 1 0 1 1 1	1 1 0 1 0 1 1 1 1

<0, 1> , <1, 1>	0 0 1 0 1 1 1 1 1	0 0 1 1 0 0 1 1 1	1 1 0 0 1 1 1 1 1	1 1 0 1 0 0 1 1 1
<1, 0> , <1, 1>	0 1 0 0 1 1 1 1 1	1 0 1 1 0 0 1 1 1	0 1 0 0 1 1 1 1 1	1 0 1 1 0 0 1 1 1

З даних таблиці 1 видно, що кожна матриця, утворена рядками, що співвідносяться з різними *d* та доповнена рядком, що складається з одиниць, є ортогональною.

Таким чином, аналіз даних таблиці 1 дозволяє зробити висновок про те, що при існуванні в матриці **Δ** рядків, що співвідносяться до двох різних *d* і наявності рядка, що містить одні лише одиниці, матриця **Δ** завжди містить в собі ортогональну підматрицю. А це, в свою чергу означає, що три втрачені основні пакети даних можуть бути відновлені, що й потрібно було довести.

3. Метод формування резервних пакетів та відновлення втрачених пакетів

Як зазначалося вище, *k* резервних пакетів Q_1, Q_2, …, Q_k пропонується формувати у вигляді лінійних комбінацій однойменних бітів основних пакетів у відповідності до формули (1). Тому проблема формування резервних пакетів зводиться до знаходження ефективного методу побудови матриці **A**, яка задовольняє умовам (2), (3) і (4).

Якщо Хемінгова відстань між будь-якою парою стовпців матриці **A** має бути згідно (3) не меншою 2-х, а кількість одиниць в кожному з стовпців цієї матриці у відповідності з (2) має бути не менше 3-х, то в якості стовпців можна вибирати *k*-розрядні двійкові коди, які містять 3, 5, 7, …,*k* одиниць.

Достатньо очевидним є той факт, що Хемінгова відстань між відмінними двійковими кодами, що мають рівну кількість одиниць, дорівнює рівно 2.

Аналогічним, очевидним є те, що Хемінгова відстань між двійковими кодами, з різницею числа одиниць в них не меншою двох, також є не меншою двох.

Оскільки, у відповідності з (4), один, наприклад перший, рядок матриці **A** складається з одиниць, то число *n* можливих стовпців, що містять 3, 5, 7, …,*k* одиниць можна обчислити у вигляді суми кількості перестановок 2-х одиниць в (*k*–1)-розрядному двійковому коді, кількості перестановок 5-ти одиниць в (*k*–1)-розрядному двійковому коді, кількості перестановок 7-ми одиниць в (*k*–1)-розрядному двійковому коді і так далі:

$$n = \sum_{j=1}^{\upsilon} C_{k-1}^{2\cdot j} \ , \tag{5}$$

де $\upsilon=(k-1)/2$ при непарному значенні *k* і $\upsilon=k/2-1$ при парному значенні *k*.

Використовуючи відомі властивості біноміальних коефіцієнтів:

$$\sum_{i=0}^{m} C_m^i = 2^m, \quad \sum_{i=0}^{m} (-1)^i \cdot C_m^i = 0,$$

формула (5) може бути трансформована до наступного вигляду:

$$n = \sum_{j=1}^{\upsilon} C_{k-1}^{2\cdot j} = 2^{k-1} - 1. \tag{6}$$

З використанням формули (6) можна визначити число *k* резервних пакетів, необхідних для відновлення трьох із *n* основних пакетів:

$$k \geq \lfloor \log_2(n+1) \rfloor + 2. \tag{7}$$

Наприклад, якщо кількість основних пакетів дорівнює n =12, то для відновлення трьох втрачених пакетів потрібно мати k = 6 резервних пакетів. Відповідно, матриця **A** формування резервних пакетів має наступний вигляд:

$$\mathbf{A}=\begin{vmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{vmatrix}.$$

При збільшенні кількості n основних пакетів ефективність резервування зростає. Наприклад, при n=120 кількість резервних пакетів становить 9, тобто 7,5% від кількості основних.

При формуванні резервних пакетів у вигляді лінійного перетворення над основними пакетами, відновлення останніх також здійснюється в результаті лінійного перетворення над основними та резервними пакетами, які не втрачені при передачі.

Процедура відновлення втраченого основного пакету при кожному варіанті втрати резервних пакетів, номери яких задаються j_1 та j_2, визначається відповідною специфікацією. Сама специфікація s_i відновлення i-го пакету $i\in\{1,2,\ldots,n\}$ являє собою $(n+k)$-бітовий вектор $s_j=\{r_1,r_2,\ldots,r_n, z_1,z_2,\ldots,z_k\}$, $\forall\ l\in\{1,2,\ldots,n\}$, $j\in\{1,2,\ldots,k\}$: r_l, $z_j\in\{0,1\}$. Відновлення i-го пакету P_i здійснюється шляхом обчислення:

$$P_i=\bigoplus_{l=1}^{n} P_l\cdot r_l \oplus \bigoplus_{j=1,\,j\neq j_1,j_2}^{k} Q_j\cdot z_j\,. \qquad (8)$$

Проведений аналіз показав, що в переважній більшості варіантів втрати резервних пакетів існує багато варіантів специфікацій для відновлення втраченого основного пакету. Цілком очевидно, що для прискорення процесу відновлення даних доцільно вибирати специфікації, що містять мінімальну кількість одиниць.

Здійснені експериментальні дослідження показали, що за рахунок оптимізації вибору процедури відновлення втрачених основних пакетів, в середньому, досягається зменшення кількості операцій логічного додавання в 1.7 рази.

Процедура відновлення втрачених при передачі основних пакетів даних за запропонованим методом може бути ілюстрована наступним прикладом в рамках використання наведеної вище матриці А при n =12 і k = 6.

При втраті, наприклад трьох пакетів, розглядається ситуація, що два з них основні, наприклад п’ятий і сьомий, тобто v=5 і w=7, а один резервний, наприклад 4-й, тобто q=4.

В цьому випадку підматриця $\mathbf{\Delta}$, що складається з стовпців матриці $\mathbf{A}$, які співвідносяться з втраченими основними пакетами та рядків, що співвідносяться з невтраченими резервними пакетами має такий вигляд:

$$\mathbf{\Delta}=\begin{vmatrix} a_{1,5} & a_{1,7} \\ a_{2,5} & a_{2,7} \\ a_{3,5} & a_{3,7} \\ a_{5,5} & a_{5,7} \\ a_{6,5} & a_{6,7} \end{vmatrix}=\begin{vmatrix} 1 & 1 \\ 0 & 0 \\ 1 & 1 \\ 0 & 0 \\ 0 & 1 \end{vmatrix}.$$

Цілком очевидно, що наведена матриця $\mathbf{\Delta}$ містить в собі ортогональну підматрицю $\mathbf{\Theta}$, яка складається з третього та п’ятого рядків матриці $\mathbf{\Delta}$:

$$\mathbf{\Theta}=\begin{vmatrix} a_{3,5} & a_{3,7} \\ a_{6,5} & a_{6,7} \end{vmatrix}=\begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix}.$$

Якщо позначити через Y_3 та Y_6, відповідно 3-тю та 6-ту складові резервних пакетів Q_3 та Q_6, то з матриці **Θ** можна скласти наступну систем лінійних рівнянь:

$$\begin{cases} Y_3 = P_5 \oplus P_7, \\ Y_6 = P_7. \end{cases}$$

Розв'язання цієї системи рівнянь надає формули для відновлення втрачених пакетів:

$$\begin{aligned} P_7 &= Y_6, \\ P_5 &= Y_3 \oplus Y_6. \end{aligned} \quad (9)$$

Для того, щоб практично відновити двійкові коди втрачених пакетів потрібно визначити значення складових Y_3 та Y_6 третього та шостого резервних пакетів, які виходячи з матриці **A** формуються у вигляді суми за модулем 2 таких складових:

$$Q_3 = P_1 \oplus Y_3 \oplus P_6 \oplus P_9 \oplus P_{10},$$
$$Q_6 = P_4 \oplus Y_6 \oplus P_9 \oplus P_{10} \oplus P_{12}.$$

Відповідно, складові Y_3 та Y_6 цих резервних пакетів можуть бути представлені у наступному вигляді:

$$Y_3 = Q_3 \oplus P_1 \oplus P_6 \oplus P_9 \oplus P_{10},$$
$$Y_6 = Q_6 \oplus P_4 \oplus P_9 \oplus P_{10} \oplus P_{12}.$$

Підставляючи отримані вирази Y_3 та Y_6 в формулу (9) для відновлення втрачених п’ятого і сьомого основних пакетів можна отримати вираз для безпосереднього відновлення вказаних пакетів у вигляді суми основних та резервних пакетів, які успішно доставлені:

$$P_7 = Y_6 = Q_6 \oplus P_1 \oplus P_6 \oplus P_9 \oplus P_{10},$$
$$P_5 = Y_6 \oplus Y_3 = Q_3 \oplus Q_6 \oplus P_1 \oplus P_4 \oplus P_6 \oplus P_{12}.$$

В підсумку, втрачені при передачі п’ятий та сьомий основні пакети можуть бути відновлені шляхом лінійних перетворень над основними та резервними пакетами, які успішно та вчасно доставлені.

Специфікації s_5 і s_7 для відновлення п’ятого та сьомого основних пакетів для розглянутого прикладу мають вигляд двох бінарних векторів ($n+k$ = 12+6 = 18), компоненти яких дорівнюють одиниці якщо відповідний основний чи резервний пакет входить в якості доданку до виразу для відновлення відповідного основного втраченого пакету:

s_7 = {1,0,0,0,0,1,0,0,1,1,0,0, 0,0,0,0,0,1},
s_5 = {1,0,0,1,0,1,0,0,0,0,0,1, 0,0,1,0,0,1}.

4. Технологія відновлення пакетів даних

Технологічно процес відновлення втрачених пакетів полягає в розв’язанні системи лінійних рівнянь, коефіцієнти якої утворені елементами ортогональної підматриці **Θ** матриці **A**. При цьому, стовпці матриці **Θ** утворені з компонентів стовпців матриці **A**, які співвідносяться з втраченими при передачі основними пакетами, а рядки – компонентами рядків, що співвідносяться з невтраченими при передачі резервними пакетами. Вище було математично строго доведено існування вказаної ортогональної матриці при виконанні умов (2), (3) і (4) для випадку, коли кількість втрачених пакетів не перевищує трьох.

Оскільки виділення з матриці **A** ортогональної підматриці **Θ** та її подальше розв’язання потребує певних часових ресурсів, що не завжди є прийнятним для систем, що працюють в реальному часі, пропонується табличний спосіб відновлення втрачених пакетів.

Спосіб полягає в тому, що на етапі налаштування системи виявляються всі можливі варіанти втрати пакетів, для кожного з цих варіантів здійснюється віднаходження ортогональної підматриці **Θ**, її розв’язання з фіксацією в табличній пам'яті формалізованого представлення специфікації дій по відновленню втрачених основних пакетів.

Загальна кількість N специфікацій, які зберігаються в табличній пам'яті визначається наступною формулою:

$$N = n \cdot (n + \frac{k \cdot (k + n - 1) + (n - 1) \cdot (n - 2)}{2}).$$

Відповідно, об'єм V пам'яті в бітах, яку займає таблиця специфікацій відновлення основних пакетів визначається формулою:

$$V = N \cdot (n + k) = \frac{n \cdot (n + k)}{2} \cdot (n + k \cdot (k + n - 1) + (n - 1) \cdot (n - 2)).$$

Дані про кількість специфікацій та потрібний для їх зберігання об'єм пам'яті для різної кількості основних пакетів наведено в таблиці 2.

Таблиця 2

Залежність кількості специфікацій гарантованого відновлення всіх основних пакетів за умови втрати не більше трьох переданих пакетів

Кількість n основних пакетів	Мінімальна кількість k резервних пакетів	Число N специфікацій	Об'єм V пам'яті специфікацій, байт
7	5	346	519
15	6	2490	6536
31	7	18460	$87 \cdot 10^3$
63	8	140742	$1.2 \cdot 10^6$
127	9	$109 \cdot 10^3$	$18.9 \cdot 10^6$
255	10	$8.59 \cdot 10^6$	$285 \cdot 10^6$

4. Висновки

В результаті проведених досліджень теоретично обґрунтовано, розроблено та досліджено метод формування резервних пакетів та їх використання для відновлення втрачених при передачі інформаційних пакетів.

Резервні пакети пропонується формувати в результаті лінійних булевих перетворень основних пакетів. Теоретично обґрунтовано спосіб формування пакетів, яких гарантує відновлення інформаційних пакетів за умови втрати не більше трьох від загальної кількості переданих пакетів. Теоретичними дослідженнями встановлена математична залежність кількості резервних пакетів від числа інформаційних.

Розроблено табличний спосіб відновлення втрачених інформаційних пакетів, який забезпечує використання теоретично мінімальної кількості операцій, за рахунок чого досягається відновлення втрачених даних.

Доведено, що запропонований метод, на відміну від відомих, дозволяє зменшити в середньому в 1,7 разів обчислювальну складність відновлення втрачених пакетів. На противагу відомим розроблений метод гарантує можливість відновлення всіх втрачених інформаційних пакетів за умови, що загальна кількість втрачених не перевищує трьох.

Список використаної літератури

1. Leong D. On coding real-time streaming under packet erasure / D. Leong, A. Qureshi, T. Ho // Proc. IEEE International Symposium Information Theory (ISIT). – Vienna. Austria. – Jul. 2013. – P. 1012-1016.

2. Стіренко С. Г. Забезпечення безперервного відтворення потокового відео в однорангових мережах з використанням erasures кодів / С. Г. Стіренко, А. В., Габінет, Ю. В. Костенко // Вісник НТУУ "КПІ". Інформатика, управління та обчислювальна техніка: збірник наукових праць. – Київ: "Век+". – 2015. – № 62. – С. 105–110.

3. Johnny M. A Multi-Lavel Encoding and Decoding Strategy for Binary Erasure Channel / M. Johnny, M. R. Aref // IEEE Transaction on Information Theory. – 2019. – Vol. 65. – No. 7. – P. 4143-4151.

4. Czap L. Secure Network Coding with Erasures and Feedback / L. Czap, C. Fragouli, V. Phabhakaran, S. Diggavi // IEEE Transaction on Information Theory. – 2015. – Vol. 61. – No. 4. – P. 1667-1686.

5. Gluesing-Luessen H. Symbol Erasure Correction in Random Network with Spread Codes / H. Gluesing-Luessen, A. L. Horlemann-Trautmann // IEEE Transaction on Information Theory. – 2019. – Vol. 65. – No. 4. – P. 2075-2091.

6. Fan X. Variable Packet-Error Coding / X. Fan, O. Kosut, A. B. Wagner // IEEE Transaction on Information Theory. – 2018. – Vol. 64. – No. 3. – P. 1530-1547.

7. Mortuza A. Parametric Approach to List Decoding of Reed-Solomon Codes Using Interpolation / A. Mortuza, M. A. Kuijper // IEEE Transactions on information theory. – Vol. 57. – № 10. – 2011. – P.6718-6728.

8. Wing Q. End-to-End Error-Correcting Codes on Networks with Wors-Case Bit Errors / Q. Wing, S. Jaggi // IEEE Transaction on Information Theory. – 2018. – Vol. 64. – No. 6. – P. 4467-4479.

9. Adler N. Burs-Erasure Correcting Codes with Optimal Average Delay / N. Adler, Y. Cassuto // IEEE Transaction on Information Theory. – 2017. – Vol. 63. – No. 5. – P. 2848-2865.

10 Bardis N. G. Usage of Linear Erasure Codes for Increasing Reliability and Efficiency of Information Delivery on the Internet / Nikolaos G. Bardis, Oleksandr P. Markovskyi, Kostiantyn V. Koliada // International Journal of Circuits, System and Signal Processing. – 2019. – Vol. 13. – P. 585-592.

References

1. Leong D., Qureshi A., and Ho T. (2013). On Coding Real-Time Streaming under Packet Erasure. Proc. IEEE International Symposium Information Theory (ISIT). Vienna. Austria. Jul. 2013. 1012-1016.

2. Stirenko S.G., and Gabinet A. V., and Kostenko J. V. (2015). Ensure Continuous Video Streaming on Peer-to-Peer Network Using Erasure Codes. Proceeding of National Technical University of Ukraine “KPI” Informatica, Control and Computer Technic. 62. 105-110.

3. Johnny M., and Aref M. R. (2019). A Multi-Lavel Encoding and Decoding Strategy for Binary Erasure Channel. IEEE Transaction on Information Theory. V.65. No.7. 4143-4151.

4. Czap L., Fragouli C., Phabhakaran V., and Diggavi S. (2015). Secure Network Coding with Erasures and Feedback. IEEE Transaction on Information Theory. V.61. No.4. 1667-1686.

5. Gluesing-Luessen H., and Horlemann-Trautmann A. L. (2019). Symbol Erasure Correction in Random Network with Spread Codes. IEEE Transaction on Information Theory. V.65. No.4. 2075-2091.

6. Fan X., Kosut O., and Wagner A. B. (2018). Variable Packet-Error Coding. IEEE Transaction on Information Theory. V.64. No.3. 1530-1547.

7. Mortuza A., and Kuijper M. A. (2011). Parametric Approach to List Decoding of Reed-Solomon Codes Using Interpolation. IEEE Transactions on information theory. V.57. No.10. 6718-6728.

8. Wing Q., and Jaggi S. (2018). End-to-End Error-Correcting Codes on Networks with Wors-Case Bit Errors. IEEE Transaction on Information Theory. V.64. No.6. 4467-4479.

9. Adler N., and Cassuto Y. (2017). Burs-Erasure Correcting Codes with Optimal Average Delay. IEEE Transaction on Information Theory. V.63. No.5. 2848-2865.

10. Bardis N. G., Markovskyi O. P., and Koliada K. V. (2019). Usage of Linear Erasure Codes for Increasing Reliability and Efficiency of Information Delivery on the Internet. International Journal of Circuits, System and Signal Processing. V.13. 585-592.