



УКРАЇНА

(19) **UA** (11) **79752** (13) **U**
(51) МПК (2013.01)
H04J 13/00

ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: u 2012 13701	(72) Винахідник(и): Яцків Василь Васильович (UA)
(22) Дата подання заявки: 30.11.2012	(73) Власник(и): ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ, вул. Львівська, 11, м. Тернопіль, 46020 (UA)
(24) Дата, з якої є чинними права на корисну модель: 25.04.2013	
(46) Публікація відомостей про видачу патенту: 25.04.2013, Бюл.№ 8	

(54) БАГАТОКАНАЛЬНИЙ АДАПТИВНИЙ ПРИСТРІЙ КОДУВАННЯ ТА ПЕРЕДАВАННЯ ДАНИХ НА ОСНОВІ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ

(57) Реферат:

Багатоканальний адаптивний спосіб кодування та передавання даних на основі системи залишкових класів містить модуль розділення даних в системі залишкових класів, модуль визначення стану каналів зв'язку; модуль адаптивного розподілу частин повідомлення; модуль передачі даних, модуль приймання даних, модуль виявлення та виправлення помилок в системі залишкових класів. Введено модуль адаптивної зміни корегуючих основ системи залишкових класів, а розподіл частин повідомлення між доступними маршрутами відбувається адаптивно в залежності від обсягу повідомлення і характеристик маршрутів.

UA 79752 U

Багатоканальний адаптивний пристрій кодування та передавання даних на основі системи залишкових класів належить до систем передавання інформації і може бути використаний в телекомунікаційних системах та комп'ютерних мережах для підвищення надійності та загальної пропускну здатності.

5 Відомий аналог - схема поширення SPREAD [1, 2], яка використовує для поділу інформації на частини порогові схеми розділення секрету з використанням алгоритмів Шаміра або Асмута-Блума [3]. Порогова схема розділення секрету (T, N) ділить інформацію на оптимальну кількість частин N . Достатньою кількістю частин N є те, що, маючи будь-яку кількість частин менше T , не можна відновити інформаційне повідомлення, в той час як, використовуючи ефективний алгоритм, можна відновити інформацію, маючи T частин з N . У схемі гібридного поширення H-SPREAD, даний метод поділу секрету використано як схема кодування.

10 Недоліком даного аналога є значне збільшення обсягу повідомлення в результаті поділу, за рахунок того, що при поділі взаємності числа P_i вибираються з умови $P_i > M$, де M - повідомлення, яке підлягає розділенню [4].

15 Найбільш близьким за технічною суттю до корисної моделі, що заявляється, є спосіб підвищення надійності передачі даних в безпроводних сенсорних мережах на основі системи залишкових класів [4], суть якого полягає у тому, що з метою підвищення загальної пропускну здатності каналів зв'язку безпроводних сенсорних мереж відбувається розділення повідомлення в системі залишкових класів і отримані залишки передаються паралельно різними доступними маршрутами.

20 В алгоритмі маршрутизації (фіг. 1) вузол безпроводної сенсорної мережі (БСМ), що ініціює передачу даних, визначає доступні маршрути, які не перетинаються (фіг. 1, бл. 1), та оцінює ефективність кожного маршруту (фіг. 1, бл. 4).

25 В залежності від кількості доступних маршрутів вибирається кількість та значення взаємності модулів p_i - (фіг. 1, бл. 2), обчислюються робочий і загальний діапазони представлення даних.

В результаті поділу повідомлення на вибрану систему модулів (фіг. 1, бл. 3) отримуємо залишки, які передаються по визначених маршрутах. Залишки більшої розрядності передаються по маршрутах з вищою оцінкою і навпаки (фіг. 1, бл. 5). Базова станція отримує підпакели (залишки по відповідних основах) і відновлює початкове повідомлення (фіг. 1, бл. 7).

30 Недоліком відомого способу є відсутність можливості зміни коректуючих властивостей кодів системи залишкових класів в процесі роботи системи передавання, що призводить до збільшення надлишковості при передачі даних, відповідно зменшення корисної пропускну здатності, за рахунок повторної передачі пакетів або передачі надлишкових даних для виявлення та виправлення помилок.

35 В основу корисної моделі поставлена задача підвищення надійності та загальної пропускну здатності каналів зв'язку безпроводних сенсорних мереж шляхом розділення повідомлення на частини в системі залишкових класів та передача частин повідомлення різними паралельними маршрутами.

40 Поставлена задача вирішується тим, що багатоканальний адаптивний спосіб кодування та передавання даних на основі системи залишкових класів, що містить модуль розділення даних в системі залишкових класів, модуль визначення стану каналів зв'язку; модуль адаптивного розподілу частин повідомлення; модуль передачі даних, модуль приймання даних, модуль виявлення та виправлення помилок в системі залишкових класів, згідно корисної моделі введено модуль адаптивної зміни корегуючих основ системи залишкових класів, а розподіл частин повідомлення між доступними маршрутами відбувається адаптивно в залежності від обсягу повідомлення і характеристик маршрутів.

45 Корисна модель ілюструється кресленням, де на фіг. 2 зображена структурна схема способу: 1 - модуль розділення даних в системі залишкових класів; 2 - модуль адаптивної зміни корегуючих основ системи залишкових класів; 3 - модуль визначення стану каналів зв'язку; 4 - модуль адаптивного розподілу частин повідомлення; 5 - модуль передачі даних; 6 - модуль приймання даних; 7 - модуль виявлення та виправлення помилок в системі залишкових класів.

Спосіб реалізується наступним чином. Повідомлення M надходить на модуль розділення даних (1) на виході якого отримуємо частини повідомлення (залишки від ділення вхідного повідомлення на основі СЗК) згідно з формулою:

$$b_i = M \bmod p_i, (1)$$

де p_i - взаємно прості числа, $p_i < p_{i+1}$.

60 Модуль 3 визначає кількість доступних маршрутів та їх характеристики (пропускну здатність, ймовірність помилки). На основі інформації з модуля 3 модуль 4 здійснює адаптивний розподіл даних, через передавальний модуль 5, в канали зв'язку. В залежності від ймовірності помилки в

каналах зв'язку, модуль 2 визначає кількість та значення корегуючих основ системи залишкових класів.

З каналів зв'язку дані надходять на модуль 6. В модулі 7 здійснюється об'єднання даних, виявлення та виправлення помилок на основі корегуючих кодів системи залишкових класів.

5 Об'єднання частин повідомлення здійснюється за формулою:

$$M = \sum_{i=1}^n b_i \cdot B_i \pmod{\varphi} \quad (2)$$

де B_i - ортогональні базиси, причому $B_i = m_i \cdot \frac{\varphi}{p_i} \equiv 1 \pmod{p_i}$; $1 \leq m_i \leq p_i - 1$,

m - вага ортогонального елемента, φ - діапазон представлення чисел,

$\varphi = \prod_{i=1}^n p_i$, n - кількість модулів системи залишкових класів.

10 Для реалізації можливості відновлення повідомлення по t частинах із n введено додаткові модулі $p_{t+1}, p_{t+2}, \dots, p_n$ - взаємно прості з будь-яким із прийнятих раніше модулів і представлено числа в системі з модулями p_1, \dots, p_n . Це означає, що передаються і виконуються операції над числами, які знаходяться в діапазоні $[0, P)$ в розширеному діапазоні $[0, \varphi)$, де $\varphi = P \cdot p_{t+1} \dots p_n$.
 15 Отже, якщо в результаті передачі отримано число більше P , це є ознакою спотворення повідомлення в процесі передачі.

Здійснено моделювання запропонованого способу в системі Матлаб і може бути використаний для підвищення надійності та загальної пропускну здатності безпроводних сенсорних мереж, зокрема при зборі та обробці мультимедійних даних.

Джерела інформації:

20 1. W. Lou, W. Liu, Y. Fang, "SPREAD: Enhancing data confidentiality in mobile ad hoc networks, IEEE INFOCOM 2004, HongKong, China, March 2004.

2. Жуков И.А., Дровозов В.И., Способы повышения надежности и безопасности сбора информации в системах управления реального времени // Проблемы информатизации та управління, 1(23). - 2008. - С. 262-276.

25 3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: Триумф, 2002. 816 с.

4. Яцків В.В. Метод підвищення надійності передачі даних в безпроводних сенсорних мережах на основі системи залишкових класів / Яцків В.В. // Радіоелектроніка та інформатика. - 2010 - № 2. - С. 32-35.

30

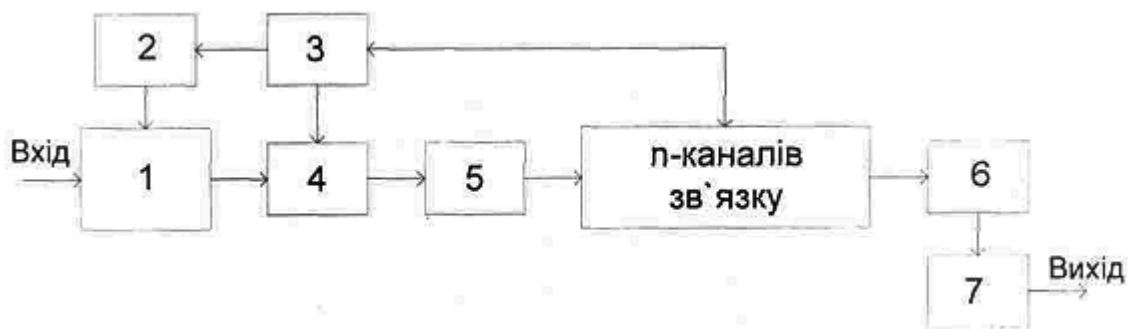
ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Багатоканальний адаптивний спосіб кодування та передавання даних на основі системи залишкових класів, що містить модуль розділення даних в системі залишкових класів, модуль визначення стану каналів зв'язку; модуль адаптивного розподілу частин повідомлення; модуль передачі даних, модуль приймання даних, модуль виявлення та виправлення помилок в системі залишкових класів, який **відрізняється** тим, що введено модуль адаптивної зміни корегуючих основ системи залишкових класів, а розподіл частин повідомлення між доступними маршрутами відбувається адаптивно в залежності від обсягу повідомлення і характеристик маршрутів.

35



Фіг. 1



Фіг. 2

Комп'ютерна верстка А. Крулевський

Державна служба інтелектуальної власності України, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601