УКРАЇНА

(19) **UA** (11) **105430** (13) **C2**

(51) МПК (2014.01)
H03M 7/00
H03M 7/18 (2006.01)
H03M 1/00
G06F 11/08 (2006.01)
G06F 11/00

ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА ВИНАХІД

(21) Номер заявки: **a 2012 13700**

(22) Дата подання заявки: **30.11.2012**

(24) Дата, з якої є чинними права на винахід: **12.05.2014**

(41) Публікація відомостей про заявку: **12.08.2013, Бюл.№ 15**

(46) Публікація відомостей про видачу патенту: **12.05.2014, Бюл.№ 9**

(72) Винахідник(и):
Яцків Василь Васильович (UA)

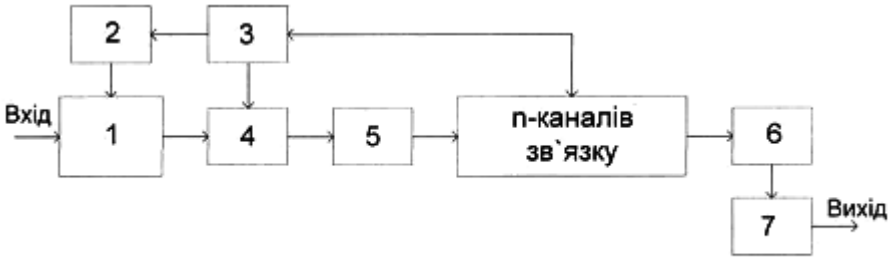
(73) Власник(и):
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ,
вул. Львівська, 11, м. Тернопіль, 46020 (UA)

(56) Перелік документів, взятих до уваги експертизою:
RU 2193276 C2; 20.11.2002;
RU 2186459 C2; 27.07.2002;
SU 1429323 A1; 07.10.1988;
RU 2300801 C2; 10.06.2007;
SU 1513620 A1; 07.10.1989;
CN 102214083 A; 12.10.2011;
JPH 199325 A; 18.04.1989;
JPH 02120898 A; 08.05.1990;

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

(57) Реферат:

Багатоканальний адаптивний пристрій кодування та передавання даних на основі системи залишкових класів належить до систем передавання інформації. Пристрій 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, 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. Запропонований спосіб дозволяє підвищити надійність передавання даних та загальну пропускну здатність.



Фіг. 2

UA 105430 C2

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 пропускної здатності.

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 меншу 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.

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

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

В алгоритмі маршрутизації (фіг. 1) вузол безпровідної 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).

В залежності від кількості доступних маршрутів вибирається кількість та значення взаємопростих 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 підпакети (залишки по відповідних основах) і відновлює початкове повідомлення (фіг. 1, бл. 7).

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

В основу винаходу поставлена задача підвищення надійності та загальної пропускної здатності каналів зв'язку безпровідних сенсорних мереж шляхом розділення повідомлення на частини в системі залишкових класів та передача частин повідомлення різними паралельними маршрутами.

Поставлена задача вирішується тим, що багатоканальний адаптивний пристрій 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 згідно винаходу 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.

Винахід 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.

Пристрій реалізується наступним чином. Повідомлення M поступає на модуль розділення даних (1) на виході якого отримуємо частини повідомлення (залишки від ділення вхідного повідомлення на основи СЗК) згідно формули:

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

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

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. 3 каналів зв'язку дані доступають на модуль 6. В модулі 7 здійснюється об'єднання даних, виявлення та виправлення помилок на основі корегуючих кодів системи залишкових класів. Об'єднання частин повідомлення здійснюється за формулою:

$$M = \sum_{i=1}^{n} b_i \cdot B_i \,(\mathrm{mod}\ \rho), \quad (2)$$

де B_i - ортогональні базиси, причому $B_i = m_i \cdot \frac{\rho}{p_i} \equiv 1(\mathrm{mod}\ p_i)$; $1 \le m_i \le p_i - 1$, m - вага ортогонального елементу, ρ - діапазон представлення чисел, $\rho = \prod_{i=1}^{n} p_i$, n - кількість модулів системи залишкових класів.

Для реалізації можливості відновлення повідомлення по t частинах із n введено додаткові модулі p_{t+1}, p_{t+2},…, p_n - взаємно прості з будь-яким із прийнятих раніше модулів і представлено числа в системі з модулями p_1, …, p_n. Це означає, що передаються і виконуються операції над числами, які знаходяться в діапазоні [0, P) в розширеному діапазоні [0, ρ), де $\rho = P \cdot p_{t+1} \cdot \ldots \cdot p_n$. 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 пропускної здатності безпровідних сенсорних мереж, зокрема при зборі та обробці мультимедійних даних.

Джерела інформації:

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., Дрововозов В.И., Способы повышения надежности и безопасности сбора информации в системах управления реального времени // Проблеми інформатизації та управління, 1(23). - 2008. - С. 262-276.

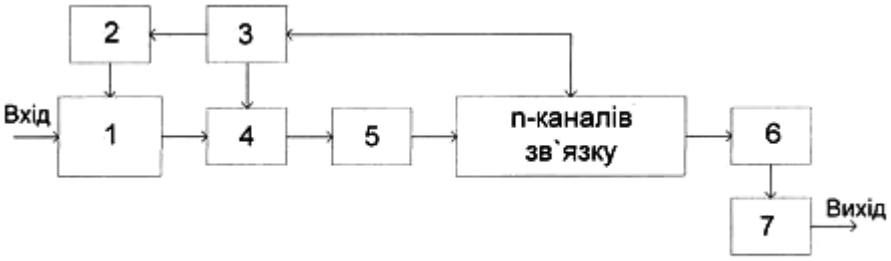
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: Триумф, 2002. 816 с.

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

ФОРМУЛА ВИНАХОДУ

Багатоканальний адаптивний пристрій 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 додатково введено модуль адаптивної зміни корегуючих основ системи залишкових класів, до входу якого підключений модуль визначення стану каналів зв'язку, а до виходу - модуль розділення даних в системі залишкових класів, при цьому модуль адаптивного розподілу частин повідомлення виконаний з можливістю розподілу частин повідомлення між доступними маршрутами, в залежності від обсягу повідомлення і характеристик маршрутів.

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