КОМП'ЮТЕРНІ ЗАСОБИ, МЕРЕЖІ ТА СИСТЕМИ

B. Shevchuk

OPERATIVE FORMATION AND COMMITTING TO A COMPACT, STABLE AND CRYPTO-CORRECTING PACKAGES OF INFORMATION IN RADIO NETWORKS

We describe the information technology of operational formation of compact and protected by covenants of information radio network.
Key words: building package, compact, crypto-resistant, noise-resistant packages of information.

Описана информационная технология оперативного формирования компактних и защищенных пакетов информации в радиосетях.
Ключевые слова: формирование пакетов, компактные, криптостойкие, помехоустойчивые пакеты информации.

Описана інформаційна технологія оперативного формування компактних та захищених пакетів інформації у радіомережах.
Ключові слова: формування пакетів, компактні, крипостійкі, завадостійкі пакети інформації.

УДК 681.31

Б.М. ШЕВЧУК

ОПЕРАТИВНЕ ФОРМУВАННЯ І ПЕРЕДАВАННЯ КОМПАКТНИХ, КРИПТОСТІЙКИХ ТА ЗАВАДОСТІЙКИХ ПАКЕТІВ ІНФОРМАЦІЇ У РАДІОМЕРЕЖАХ

Вступ. Пакетна передача інформації отримала широке застосування в персональних, сенсорних, локально-регіональних та глобальних комп'ютерних мережах, не залежно від типу середовища передачі різноманітних даних. Середовищем може бути оптоволоконний чи кабельний канал зв'язку, радіоканал, лазерний канал, гідроканал, енергетичні лінії та ін. З розвитком елементної бази і технологій передачі пакетів інформації у безпроводових мережах, освоєння нових діапазонів частот та розробка ефективних протоколів функціонування децентралізованих мереж з самоорганізацією передачі даних забезпечуються умови для широкого проникнення радіотехнологій у галузі побудови перспективних комп'ютерів, промислових, медичних і побутових (домашніх) систем і мереж, мереж персонального, локально-регіонального та глобального зв'язку. Найбільш динамічно розвиток пакетних радіомереж широкого застосування розвивається в напрямку побудови mesh-мереж (осередкових мереж) з повною децентралізацією функцій керування маршрутом передачі пакетів у неліцензійному діапазоні частот. За рахунок такої технології mesh-мережа володіє високою живучістю (відмовостійкістю), з'єднуючи свої вузли навіть у випадку виходу з ладу більшості з них. Сучасні системи WiFi, які працюють у діапазонах 2.4 і 5 ГГц, забезпечують високошвидкісну пакетну передачу даних (напри-

клад, стандарт IEEE 802.11n забезпечує швидкість передачі даних до 480 Мбіт/с) при побудові ad hoc- і mesh-мереж з альтернативними маршрутами доставки інформації між вузлами. В середині 2011 року на ринку мережевих рішень з'явився чіпсет радіотехнології WiGig AR9004TB, розрахований на роботу в трьох діапазонах частот: 60, 5, 2.4 ГГц. Нова радіотехнологія, яка регламентується стандартом IEEE 802.11ad (WiGig-стандарт), забезпечує передачу пакетів даних у діапазоні частот 60 ГГц на невеликі відстані зі швидкістю до 7 Гбіт/с (стандарт IEEE 802.11ac регламентує передачу даних на більш дальні відстані зі швидкістю 1 Гбіт/с). Підвищення ефективності функціонування перспективних та діючих пакетних радіомереж досягається за рахунок комплексної обробки та кодування даних (вимірювальних сигналів, рухомих і нерухомих відеоданих, різноманітних масивів (файлів) даних) у місцях їх утворення, тобто безпосередньо на абонентських системах (станціях) комп'ютерних мереж. Основою комплексної обробки та кодування даних на абонентських системах (АС) мереж є математичні методи оперативної фільтрації-стиску сигналів та зображень з урахуванням введення і компактного кодування достовірних та інформативних відліків обвідних сигналів (відеосигналів), компактного кодування масивів даних, криптостійкого та завадостійкого кодування даних, що підлягають передачі по каналам зв'язку та накопиченню у базах даних і запису на електронні носії. При цьому важливо оптимізувати процес обробки і кодування даних на АС як за швидкістю і точністю кодування даних, так і з урахуванням досягнення заданих величин ступеня захисту інформації у мережі та підтримки поточного рівня захисту даних від спотворень канальними завадами.

Мета роботи – розробка методології реалізації швидкодіючої комплексної обробки та кодування даних на АС радіомереж у процесі формування та передавання компактних, псевдохаотичних та захищених пакетів інформації. Формування компактних пакетів інформації орієнтоване на суттєве зменшення кількості пакетів (транзакцій або циклів встановлення зв'язку та передачі пакетів між парами абонентів), що передаються або ретранслюються між абонентами мережі, та на передачу великих масивів (файлів) даних одним або мінімальною кількістю криптостійких та завадостійких пакетів. Передача псевдохаотичних та захищених пакетів передбачає передачу беззбиткових криптостійких і завадостійких даних за відкритими каналами зв'язку з завадами. Оперативна реалізація запропонованих ключових операцій з обробки і кодуванню даних на АС є основою для побудови інформаційно-ефективних радіомереж [1, 2] широкого застосування.

Функціонування багатокоміркових сенсорних та локально-регіональних радіомереж грунтується на роботі комірки (рис. 1), яка забезпечує передачу інформаційних пакетів (ІП) з топологією "кожний з кожним", при цьому передача інформації від однієї АС до іншої може здійснюватись за різними маршрутами. Це дозволить будувати різноманітні розподілені мережі (кластерне дерево, багатокоміркова мережа) з надійною передачею інформації на великі відстані. Для покриття зв'язком великих територій із коміркових мереж формуються кластери, в яких один із абонентів виконує функції "вершини" кластеру, який у свою

чергу забезпечує зв’язком підвищеної дальності з “вершинами” сусідніх кластерів. Таким чином, у залежності від відстані між абонентом-відправником ІП та абонентом-приймачем ІП маршрутизація пакетів здійснюється на рівні комірки, багатьох комірок (кластеру), багатьох кластерів.

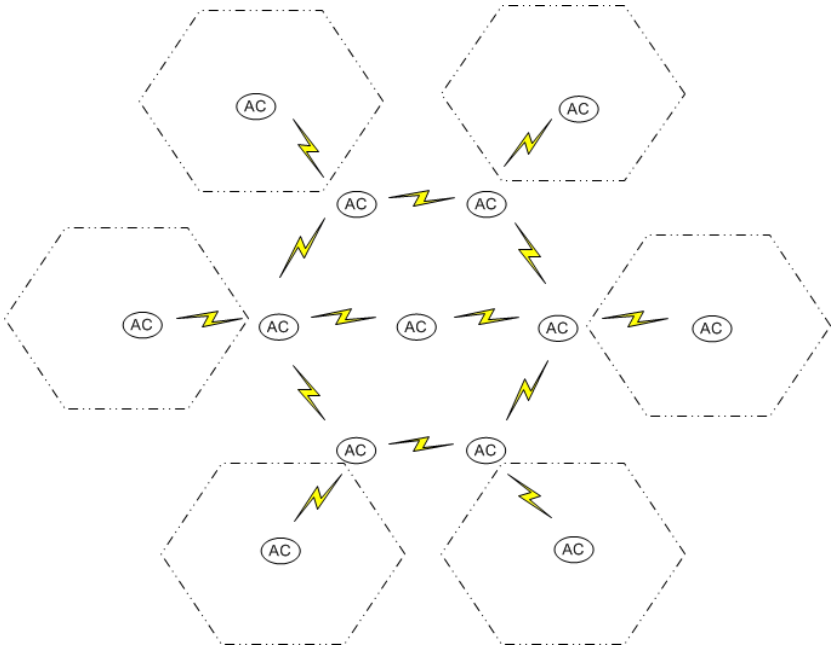


РИС. 1. Структура коміркової радіомережі

У традиційних mesh-мережах всі АС мережі поділяються на об’єктні АС, що встановлюються в місцях зародження інформаційних потоків і часто є мобільними, та стаціонарні або мобільні абоненти-ретранслятори (маршрутизатори, точки доступу, routers). У сенсорних мережах об’єктні АС, як правило, є малогабаритними пристроями з автономним живленням з тривалістю неперервної роботи місяці-роки. Маршрутизатори встановлюються на пріоритетних висотах та підтримують зв'язок як з віддаленими маршрутизаторами, так і з підзвітними об’єктними АС. При необхідності передачі інформації від *j*-ї АС до *i*-ї АС базова процедура передачі ІП здійснюється в такій послідовності дій віддалених АС: 1) *j*-та АС передає у радіоканал пакет-запит ”Хто знає як зв’язатись з *i*-ю АС”; 2) маршрутизатори ретранслюють даний пакет один одному і запам’ятовують маршрут, включаючи адреси проміжних маршрутизаторів, а також рівні сигналів у каналах зв’язку, за якими передається цей запит. Процес передачі пакета-

запиту продовжується до тих пір поки *i*-та АС не отримає даний запит. Ймовірно, що *i*-та АС отримає запит за декількома маршрутами, тому за рівнями сигналів вибирається самий надійний маршрут; 3) *i*-та АС передає *j*-й АС пакет-відповідь з оптимальним маршрутом доставки інформації; 4) *j*-та АС та *i*-та АС здійснюють передачу пакетів даних за визначеним маршрутом. Якщо одна із АС переміщується чи виходить із ладу проміжний маршрутизатор, то маршрут передачі ІП періодично коректується, тобто повторюються послідовності дій 1 – 4. При великій кількості мобільних АС необхідне постійне позиціювання активних абонентів у мережі. У випадку використання центральної станції (ЦС) (координатора мережі) позиціювання мобільних АС здійснюється централізовано. Наприклад, періодично кожний абонент передає ЦС свої координати, визначені за допомогою GPS системи. В іншому випадку ЦС періодично запитує у всіх маршрутизаторів адреси "підзвітних" активних АС. Отримавши множину пакетів-відповідей ЦС пропонує віддаленим АС оптимальні шляхи доставки інформації як до себе так і між віддаленими абонентами. При цьому кожний маршрутизатор передає інформацію не всім сусіднім маршрутизаторам, а тільки тим, з якими є надійний зв'язок. На сьогоднішній день у мережах MANET (Mobile Ad hoc Network), які є децентралізованими повнозв'язковими мережами з багатьма альтернативними шляхами передачі пакетів між АС, протоколи маршрутизації ІП базуються на побудові таблиць маршрутизації для кожної АС-ретранслятора. Таблиці маршрутизації будуються на основі реалізації вектора відстані або стану зв'язку. При наявності m проміжних маршрутизаторів (М) між віддаленою парою абонентів, що передають ІП (наприклад, згідно прийнятої за основу методології маршрутизації у процесі передачі ІП утворюється ланка абонентів $AC_j \leftrightarrow M_1 \leftrightarrow M_2 \leftrightarrow \ \ldots \ M_m \leftrightarrow AC_i$), середня швидкість передачі інформації залежатиме від якості проміжних каналів зв'язку (поточних енергетичних показників співвідношення сигнал/шум у каналі).

Поточна швидкість передачі інформації у проміжних каналах зв'язку з робочою смугою F_k (k = 1, …, m + 1) залежить від тривалості кожного бітового символу T_b^k k-го ІП, де $T_b^k = 1/2F_k$, сумарного коефіцієнта стиснення даних K_c^i i-ї АС, що формує і передає ІП, а також від величини бази B_s^k s-го бітового символу k-го ІП, де s = 1, …, N^k, N^k – максимальна кількість бітових символів k-го ІП, включаючи символи синхропослідовності, початку ІП, поля адреси, поля керування, інформаційного кадру, перевіркового коду та ознаки завершення ІП. Для реалізації надійного прийому бітових символів інформаційного кадру ІП необхідно виділити синхропослідовності, визначити початок ІП і на основі отриманої інформації у відповідні моменти часу, наприклад, по завершенню поточного бітового інтервалу, визначити значення бітів службових даних і інформаційного кадру. Відповідно, при заданій довжині інформаційного кадру тривалість ІП суттєво залежить від способу захисту даних від завад. Оптимальне вирішення цієї проблеми полягає у реалізації на АС перемішування даних, оперативного завадостійкого кодування бітів ІП та передачі перевіркових бітів ІП

шумоподібними сигналами (ШПС) з базою B_{pk}^{k}, яка перевищує мінімально необхідну базу ШПС $B_{\min}$ [2]. Враховуючи, що $N^k = N_i^k + N_{sr}^k + N_{pk}^k$, де N_i^k – кількість бітів інформаційного кадру ІП, N_{sr}^k – сумарна кількість біт службових даних ІП, включаючи перевіркові коди службових даних, N_{pk}^k – кількість біт перевіркового коду ІП, поточна швидкість передачі ІП у моноканальній радіомережі визначається виразом

$$R_i = \frac{K_c}{k_s \cdot T_{ip}^k / N^k} = \frac{K_c}{k_s \left[\left(N_i^k + N_{SR}^k\right) \cdot B_{\min} + N_{pk}^k \cdot B_{pk}\right]}, \qquad (1)$$

де K_c – сумарний коефіцієнт стиснення даних; k_s – коефіцієнт, що враховує якість відновлення фронтів цифрових сигналів; T_{ip}^k – тривалість *k*-го ІП; B_{pk} – база ШПС перевіркового коду ІП, $B_{pk} > B_{\min}$.

Таким чином, реалізація надійної та високошвидкісної передачі ІП в радіомережах без суттєвого ускладнення радіотехнічного обладнання АС досягається за рахунок ретрансляції пакетів з урахуванням наявності альтернативних маршрутів передачі даних, компактного, криптостійкого та завадостійкого кодування даних безпосередньо в місцях їх виникнення. При цьому в процесі встановлення зв'язку сусідні абоненти мають визначати стан каналу та вибирати необхідну величину $B_{\min}$ [2].

Формування компактних ІП забезпечується за рахунок виконання процесорами АС мережі адаптивних алгоритмів стиснення сигналів (відеосигналів) з допустимими (контрольованими) втратами несуттєвої інформації та адаптивних алгоритмів стиснення даних без втрат. У процесі стиснення даних з допустимими втратами в найбільш швидкодіючому алгоритмі кодування сигналів (відеосигналів) визначають амплітудно-часові характеристики суттєвих відліків-екстремумів (СВ-Е) та проміжних СВ, які визначають на пологих ділянках сигналів через певний інтервал часу, величина якого залежить від мінімально необхідного коефіцієнта стиснення даних $K_{c\min}$. При цьому для більш компактного кодування СВ-Е та проміжних СВ, в залежності від прикладних завдань та вимог до точності відновлення огинаючих сигналів (відеосигналів) відповідні СВ доцільно кодувати з використанням мінімальної $q_{\min}$ або максимальної $q_{\max}$ кількості біт відліків СВ. При наявності сусідніх СВ-Е деякі з них можуть ігноруватись. У більш точному алгоритмі визначають СВ-Е та точки перегину (СВ-ТП), а також проміжні СВ. При цьому в обох випадках суттєві відліки кодують кількістю біт $q_{\min}$ або $q_{\max}$ у залежності від опосередковано визначеної величи-

ни сигнал/шум в околиці СВ [1]. Для прискорення обробки і кодування даних СВ-ТП визначають лише на менш динамічних ділянках огинаючих сигналів, для яких виконується умова $\Delta X_i^F \le \Delta X_d$, де ΔX_i^F – поточна різниці між сусідніми вхідними відліками відфільтрованого сигналу, ΔX_d – допустима крутизни сигналу, а частоту опиту сигналу f_0 підбирають адаптивно, в залежності від поточної крутизни сигналу: $f_0 = f\left(\Delta X_i^F\right)$. Таким чином, у процесі обробки і кодування відліків поточної вибірки сигналу (відеосигналу) визначають амплітудно-часові параметри відфільтрованих *i*-х відліків сигналу ΔX_i^F та відповідний їй коефіцієнт проріджения k_p вхідної вибірки даних для визначення параметрів наступного відфільтрованого відліку ΔX_{i+1}^F. З метою забезпечення максимально компактного кодування даних та точного відновлення огинаючої сигналу при її різних динамічних і хаотичних діях доцільно адаптивно змінювати коефіцієнт k_p, а також комбінувати алгоритми точного та менш точного (швидкодіючого) кодування даних. Вихідні компактні потоки даних кодуються у вигляді наступного потоку даних:

$$\begin{aligned}
&\left\{CI_z\right\}\left[\left\{CI_{pa}^1\right\}\left\{\left(KD_{CB}^{11}\right)\left(KD_{CB}^{12}\right)...\left(KD_{CB}^{1N_1}\right)\right\}\right]... \\
&...\left[\left\{CI_{pa}^2\right\}\left\{\left(KD_{CB}^{21}\right)\left(KD_{CB}^{22}\right)...\left(KD_{CB}^{2N_2}\right)\right\}\right]... \\
&...\left[\left\{CI_{pa}^n\right\}\left\{\left(KD_{CB}^{n1}\right)\left(KD_{CB}^{n2}\right)...\left(KD_{CB}^{nN_n}\right)\right\}\right],
\end{aligned}$$

де CI_z – загальна службова інформація; CI_{pa} – службова інформація параметрів адаптації; KD_{CB}^{ij} – компактні дані *j*-го СВ *i*-ї вибірки вхідних даних, $i = 1, \ldots, N_j$, $j = 1, \ldots, n$; N_i – максимальна кількість СВ *i*-ї вибірки вхідних даних.

У процесі стиснення даних без втрат, враховуючи природну нерівномірність слідування *l*-бітових послідовностей ($l \ge 4, 5, 6, ...$) у масиві стислих даних з доступними втратами, доцільно за *m* каналами аналізу даних ($m \ge 1$) визначити відповідні *l*-бітові послідовності, які найчастіше зустрічаються, визначити канал аналізу даних, який найбільш компактно кодує дані з наступним виконанням операцій заміщення двійкових послідовностей. Послідовне виконання вищеописаних операцій стиснення даних з допустимими втратами і без втрат інформації є основою для реалізації надвисокого стиснення даних засобами АС комп'ютерних мереж.

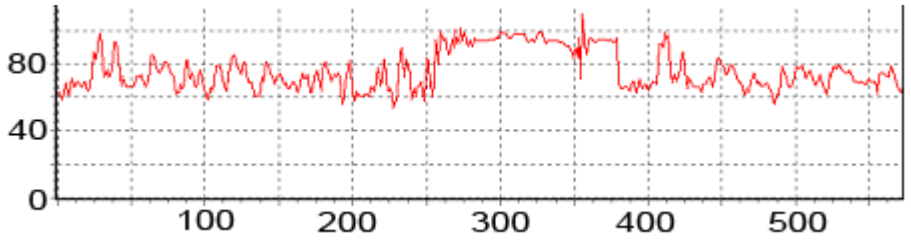
Формування крипостійких ІП абонентами мережі досягається на основі взаємної аутентифікації абонентів, використанні одноразових шифрів у процесі криптографічного кодування даних поточного ІП та динамічної зміни і розподілу секретних ключів. Саме розподіл ключів та їх динамічна зміна є ключовою

проблемою організації ефективного захисту даних у мережах. Оптимальне вирішення проблем захисту даних у мережах (взаємна аутентифікація абонентів, шифрування даних, динамічний розподіл ключів) досягається за рахунок реалізації абонентами мережі криптографічного кодування даних з відкритим ключем. При цьому секретний ключ відомий тільки даному абоненту, а відкритий ключ надається кожному абоненту мережі (може бути розміщений на Web-сайті або переданий засобами мережі). Відповідно, криптографія з відкритим ключем забезпечує ефективні механізми аутентифікації і шифрування та надає можливість використати спрощені методи розподілу відкритих ключів. Серед вимог, які пред'являються до методів шифрування пакетів інформації з відкритим ключем, необхідно виділити наступні [3]: пара "секретний ключ – відкритий ключ" має бути рівноправною з криптографічної точки зору (наприклад, абонент, який передає ІП, може зашифрувати дані за допомогою відкритого ключа, а абонент, який приймає пакет, використовує свій секретний ключ, щоб розшифрувати дані. Можливий протилежний варіант: абонент що передає пакет, зашифровує дані за допомогою свого секретного ключа, а абонент, який приймає пакет, за допомогою відкритого ключа дешифрує дані; оскільки кожний абонент приховує свій секретний ключ від інших абонентів, виключаючи можливість несанкціонованого дешифрування зашифрованої інформації, то абонент, що передає пакет, має використовувати відкритий ключ для шифрування даних перед їх передачею, а для дешифрування даних використовує секретний ключ, який відповідає відкритому ключу. Для реалізації ефективної аутентифікації [3], абонент, що передає у пакеті відповідне повідомлення, наприклад, номер станції, шифрує дані пакету з використанням секретного ключа. Абонент, що приймає пакет, дешифрує повідомлення за допомогою відповідного відкритого ключа. Якщо дешифроване за допомогою відкритого ключа повідомлення відповідає попередньо заданому, то приймальна станція вважає передавальну станцію легітимною. Шифрування відповідного повідомлення (номеру станції) виконує роль цифрового підпису.

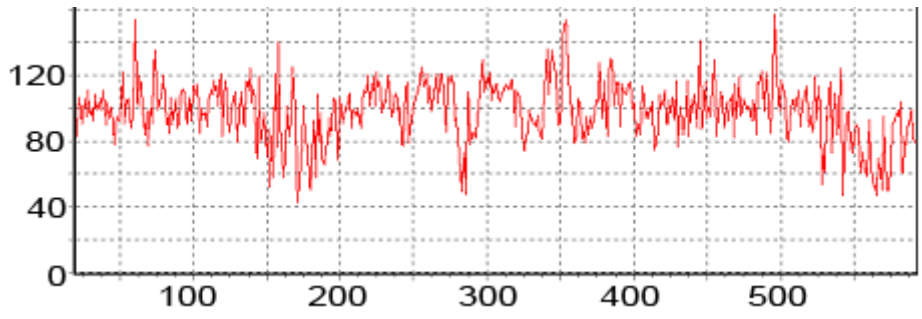
Основою криптографічного шифрування ІП є генерація парою абонентів "відправник ІП – приймач ІП" довготривалих псевдовипадкових послідовностей (ПВП), які від пакету до пакету є різними, та виконання операцій гаміювання відповідних даних [1, 2]. У результаті в канал зв'язку відправляються псевдохаотичні сигнали, параметри яких від пакету до пакету є різними. На рис. 2, а – в показано зображення та відповідні відеосигнали, які підлягають обробці та кодуванню (на рис. 2, б – відеосигнал середнього рядку, на рис. 2, в – самого нижнього). На рис. 3 показано розподіл q-бітових символів (q = 8) стислого та зашифрованого зображення Львівських Карпат, яке наближене до рівномірного. На рис. 4, а, б показано хаосграми закодованого масиву відеоданих (залежність попереднього символу від наступного) для q = 8 (рис. 4, а) і q = 7 (рис. 4, б).

Наведені результати досліджень підтверджують хаотичність псевдовипадкових даних, які відправляються в канал зв'язку.

а



б



в

РИС. 2. Львівські Карпати та відповідні фрагменти огинаючих відеосигналів

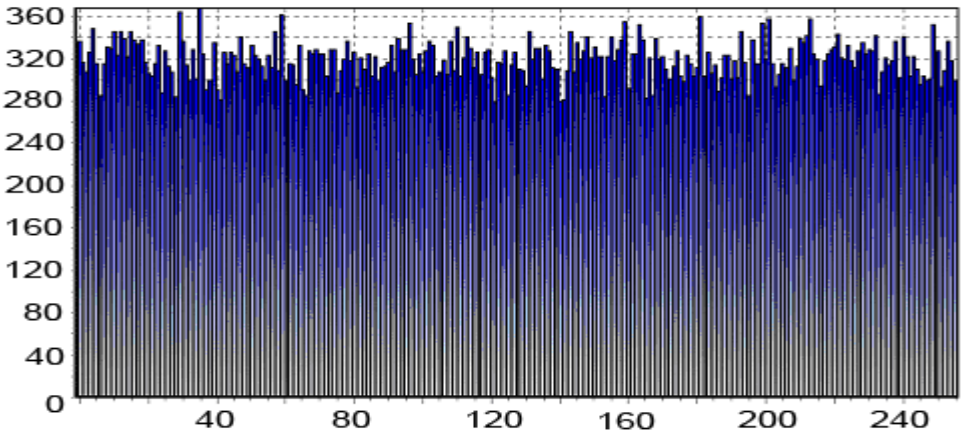
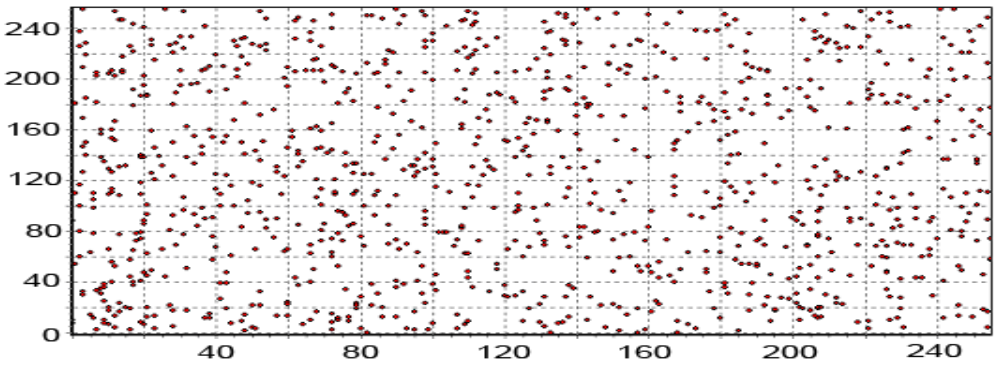
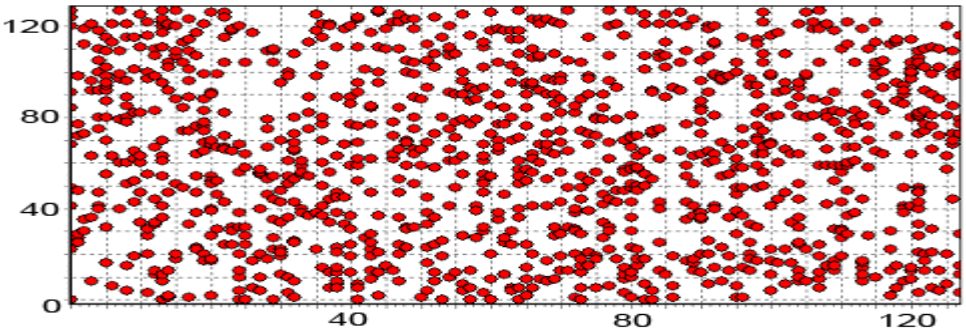


РИС. 3. Розподіл q-бітових символів (q = 8) зашифрованого зображення



а



б

РИС. 4. Хаосграми закодованого відеозображення

Формування завадостійких ІП досягається за рахунок комбінації кодування бітів ІП з використанням ПВП, наприклад, кодів поля Галуа, з формуванням сигнальних коректуючих послідовностей [4] та передачі перевіркових кодів шумоподібними сигналами.

Важливою проблемою при передачі ІП є вирішення безконфліктної передачі пакетів у режимі множинного доступу абонентів до спільного ресурсу мережі – радіоканалу. Ефективне вирішення цієї проблеми досягається за рахунок розподілу абонентів на групи пріоритетності та багатоциклового формування конфліктуючими абонентами випадково-зменшуючих інтервалів [1]. За рахунок цього реалізується процедура децентралізованого керування безконфліктною передачею ІП, при якій першими в радіоканал передають ІП ті абоненти, які відносяться до більш пріоритетної групи та мають більш пріоритетний номер у групі.

Висновки. Запропонована технологія формування компактних, криптостійких та завадостійких пакетів інформації у радіомережах з децентралізацією маршрутизації ІП суттєво підвищує ефективність передачі інформації за рахунок зменшення сумарної кількості пакетів, що підлягають передачі в радіоканалах. Подальшим напрямком підвищення ефективності функціонування радіомереж є реалізація абонентами мережі надвисокого стиску-захисту даних.

1. *Шевчук Б.М., Задірака В.К., Гнатів Л.О., Фраєр С.В.* Технологія багатофункціональної обробки і передачі інформації в моніторингових мережах. – К.: Наук. думка, 2010. – 370 с.
2. *Шевчук Б.М.* Оброблення, кодування та передавання даних засобами абонентських систем інформаційно-ефективних радіомереж // Комп'ютерні засоби, мережі та системи. – 2010. – № 9. – С. 130 – 139.
3. *Гейер Д.* Беспроводные сети. Первый шаг: Пер. с англ. – М.: Издательский дом "Вильямс", 2005. – 192 с.
4. *Николайчук Я.М., Воронич А.Р., Гринчишин Т.М.* Теоретичні основи, принципи формування та передавання інформації на основі сигнальних коректуючих кодів // Матеріали проблемно-наукової міжгалузевої конф. "Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління (ПНМК-2010)". – Бучач: Бучачський інститут менеджменту і аудиту, 2010. – Вип. 6. – **1**. – С. 41 – 48.

Отримано 15.09.2011