

# СПОСОБИ ВИКОРИСТАННЯ ВІЛЬНИХ БЛОКІВ У КАДРІ УПРАВЛІННЯ ДОСТУПОМ ДО СЕРЕДОВИЩА ПЕРЕДАЧІ ПРИ РОЗПОДІЛІ КАНАЛЬНИХ РЕСУРСІВ

Дробяз М.О., Коляденко Ю.Ю.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,  
Харківський національний університет радіоелектроніки,  
Україна

E-mail: [mykhailo.drobiaz@nure.ua](mailto:mykhailo.drobiaz@nure.ua),  
[yuliia.koliadenko@nure.ua](mailto:yuliia.koliadenko@nure.ua)

---

## Abstract

*To prevent interference to the operation of the primary user (PU), communication devices using cognitive services and DSA techniques can transmit and receive information only when there is no obvious interference to the operation of the PU. If this condition is met, there is no need to hard limit the transmission power for the virtual secondary user (SU). Let each SU node be equipped with one receiver and a radio module for processing control signals. The receiver works on a software platform and can be configured with various parameters such as transmission power, frequency, modulation type and data rate. Since SUs use different frequency channels, this can lead to a problem of lack of interaction between neighboring SUs, where two nodes cannot communicate with each other if they operate on different radio frequency channels, this results in an additional load on the SU.*

---

Для запобігання перешкод роботі первинного користувача (PU), засоби зв'язку, що використовують когнітивні служби та техніки DSA, можуть передавати та приймати інформацію тільки тоді, коли немає очевидних перешкод для роботи PU. При дотриманні цієї умови немає потреби жорстко обмежувати потужність передачі для віртуальних вторинних користувачів (SU).

Нехай кожен вузол SU у вигляді SDR обладнаний одним приймачем та радіомодулем для обробки сигналів управління. Приймач працює на програмній платформі і може бути налаштований з різними параметрами, такими як потужність передачі, частота, вид модуляції та швидкість передачі даних. Оскільки SU використовують різні частотні канали, це може привести до проблеми відсутності взаємодії між сусідніми SU, коли два вузли не можуть зв'язатися один з одним, якщо працюють на різних радіочастотних каналах, це призводить до додаткового навантаження на SU [3].

Загальний канал управління когнітивного радіо (КР) для найбільш складного випадку позасмугової реалізації може автоматично використовувати низькочастотний діапазон радіочастотного спектра (РЧС), на ділянці частот, які можуть сприяти передачі сигналу на великі відстані, але з іншого боку, мати низькі швидкості передачі. Далі розглядається загальний канал управління за допомогою спеціального управляючого радіопередавача, щоб гарантувати, що повідомлення управління можна отримати вузлами, попри невідповідність між смугами частот [1]. Для підтримки роботи КР пропонується використовувати розширену схему кадру RTS/CTS на основі протоколу MAC-рівня стандарту IEEE 802.11. Для цього слід модифікувати зарезервовані осередки в кадрах RTS/CTS/FC перенесення додаткової інформації, як показано на рисунку 1.

Кадр запит на відправку надсилається передавачем по каналу управління шляхом ширококомовного розсилання. Для когнітивної мережі пропонується додати у кадр RTS список вільних каналів, допустиму довжину кадру приймання-передачі та пріоритет переданого трафіку, що сукупно виставляються приймачем-передавачем. У полі VCL міститься список тимчасово невикористовуваних каналів, які можуть використовуватися для передачі даних.

Поле «Довжина» вказує розмір пакета передачі в байтах, а поле «Пріоритет» вказує на пріоритет пакету, що передається, голос, передача даних, відео-дзвінок, вказаний PE3 SU під час передачі даного кадру. Кадр дозволу відправки – надсилається приймачем канал управління після прийому RTS.

Пропонується модифікувати поле «Вибраний канал», який має містити ідентифікатор каналу, який повинен використовуватись для подальшої передачі, поле «Потужність», яке має містити значення потужності, що випромінюється передавачем, поле «Швидкість передачі даних», яке має містити інформацію про швидкість передачі даних, що підтримується.

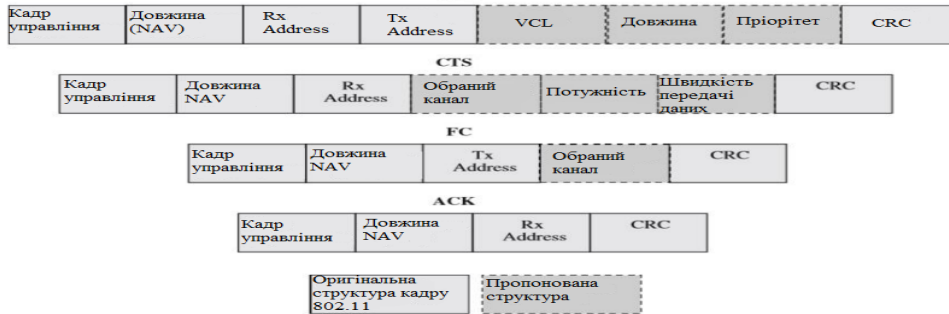


Рис. 1. Структура кадрів управління 802.11, запропонованих для застосування у каналі управління когнітивних мереж

Кадр зі списком частот містить дані про зміні частоти виділеного для прийому-передавача SU, і присутній у структурі кадру через зміну частоти після прийому RTS-кадру. Кадр підтвердження – кадр відправляється приймачем на канал даних після успішного отримання кадру даних від відправника та не модифікується. Оскільки когнітивні служби можуть використовувати різні стандарти радіозв'язку та безпроводової передачі, особливістю стандарту IEEE 802.11af є використання вектора розподілу мережі, який є програмним лічильником часу, необхідного для передачі попереднього кадру. На рисунку 2 представлена схема обміну сигнальними повідомленнями між одержувачем та відправником у рамках IEEE 802.11af.

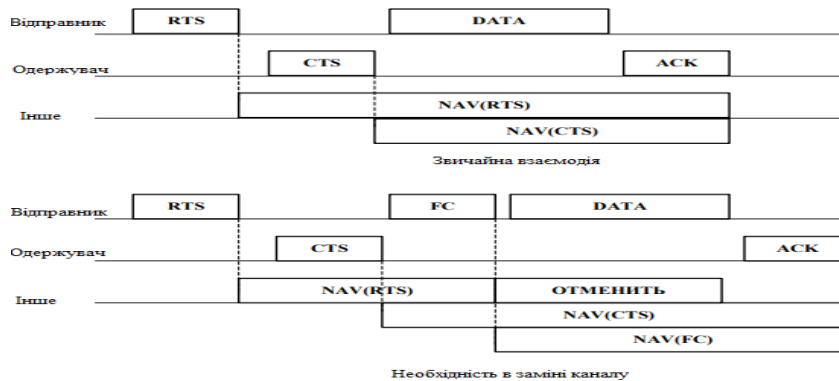


Рис. 2. Схема обміну сигнальними повідомленнями у штатному стані та при зміні робочих каналів

Тут можуть використовувати значення NAV, що допомагають в рамках когнітивної мережі контролювати заняття каналу, що необхідно передачі даних. Подана схема передбачає два стани: стан нормальної взаємодії та стану зміни частоти [4]. Під станом зміни частоти розуміється відправлення повідомлення зі списком частот FC, в якому міститься запис про частоту нової несучої у зв'язку, наприклад, з початком роботи PU. Перед початком передачі даних когнітивне РЕЗ перевіряє інформацію про каналів та створює список каналів VCL, як показано на рисунку 3, що складаються з каналів із NAV=0.

Потім кадр VCL інкапсулюється в кадр RTS. Усі найближчі вузли – когнітивні РЕЗ – приймають кадр RTS, далі зберігають відомості про ширококомовний канал і пов'язаний з ним NAV у кеш-пам'яті інформації про канал. Після того, як вузол-одержувач успішно приймає кадр RTS, відбувається відновлення кадру даних та визначається граничне значення сигнал/шум, і далі виконується оцінка інтерференції.

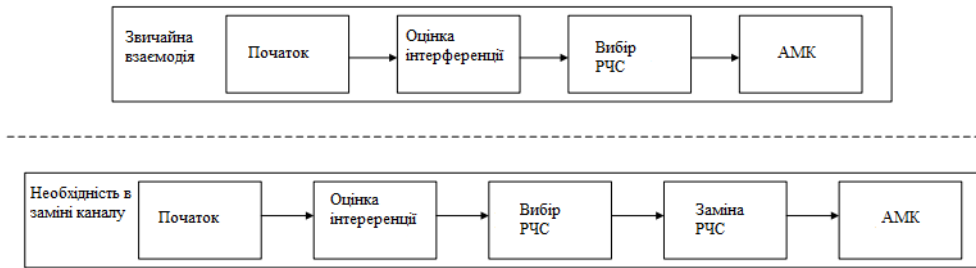


Рис. 3. Послідовність обміну для створення списку каналів

У зв'язку із суттєвою затримкою, що виникає при перемиканні, доцільно застосовувати метод адаптивного кодування. Метод АМК забезпечує захист інформації за наявності шуму у каналі. Далі приймач когнітивного РЕЗ визначає значення поля NAV кадру CTS, щоб врахувати затримку під час перемикання каналу. Потім приймач створює кадр CTS з вибраним каналом, необхідної потужності та підтримуваної швидкістю передачі [2]. Коли кадр CTS прийнято, то вузол перевіряє поле «Вибраний канал», щоб визначити номер каналу передачі даних. Якщо необхідно виконати перемикання каналів, передавач перекине кадр FC загальному каналу управління; кадр містить дані про новий робочий канал. Коли кадр FC отримано, вузол-одержувач оновлює вміст пам'яті (кеш-пам'яті) з інформацією про робочий канал, щоб скасувати NAV, згенерований початковим кадром RTC і встановити новий NAV. Після надсилання кадру FC передавач виконує перемикання поточного каналу і передає кадр даних нового робочого каналу.

Отже, для оперативного обміну інформацією про стан та наявність вільних каналів, запропоновано модифікувати вміст кадрів управління 802.11 для когнітивної мережі, де пропонується додати до кадру RTS список вільних каналів, допустиму довжину кадру приймання-передачі та пріоритет переданого трафіку, у кадрі CTS модифікувати поле «Вибраний канал», яке має містити ідентифікатор робочого каналу когнітивної мережі у полі «Потужність» передавати значення потужності, що випромінюється передавачем когнітивного радіоелектричного засобу.

## Література

1. Гур'янов, І.О. Когнітивне радіо: нові підходи до забезпечення радіочастотним ресурсом перспективних радіотехнологій. Електров'язок, 2012 №8. 8с.
2. Дробяз М.О., Коляденко Ю.Ю. Аналіз розвитку мереж зв'язку з застосуванням когнітивних технологій. Збірник тез доповідей. Харків, 2023.с.13-15
3. Дробяз М.О., Коляденко Ю.Ю. Метод зменшення часу доступу до каналу передачі в когнітивній мережі. 27-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті». Зб. матеріалів форуму. Т.4. Харків, 2023. с.13-14.
4. Салієва О.В., Яремчук Я.Є. Розробка когнітивної моделі для аналізу впливу загроз на рівень захищеності комп'ютерної мережі. Реєстрація, зберігання і обробка даних. 2019. Т. 21. № 4.с.28-39.