УДК 621.3

Р.С. Колодій, О.В. Тимченко
Національний університет "Львівська політехніка"

МЕТОДИ ПОБУДОВИ СЕНСОРНИХ МЕРЕЖ МОБІЛЬНОГО МОНІТОРИНГУ ЕКГ

Розглянуто методи побудови та особливості реалізації сенсорних мереж для потреб телемедицини, зокрема мобільного моніторингу електрокардіограми пацієнтів. Показано шляхи вирішення проблем, пов'язаних з обмеженим енергоспоживанням та мобільною топологією таких мереж.

The methods of construction and realization of sensory networks are examined for the necessities of tele medecine, in particular mobile monitoring of electrocardiogram of patients. The ways of decision of problems, related to the limited energy consumption and mobile topology of such networks are rotined.

Вступ

Донедавна сенсорні мережі вважалися хоча і дуже перспективною, але лишень експериментальною технологією. Сьогодні пристрої, що працюють за радіопротоколом ZigBee, мають все необхідне для швидкого розповсюдження сенсорних радіомереж: сенсори з вбудованим цифровим інтерфейсом, дешеві мережеві пристрої з вбудованими функціями маршрутизації і декілька технологій для створення мереж.

Об'єднані у безпровідну мережу сенсори можуть відстежувати параметри навколишнього середовища або фізіологічні показники людини. Моніторинг може здійснюватися на дуже великій території, тому що сенсори передають інформацію «ланцюжком» – від сусіда до сусіда. Технологія дає їм змогу роками (навіть десятиліттями) працювати без заміни батарей.

Проте обчислювальні ресурси вузлів сенсорної мережі доволі обмежені. Для економії енергії вузли майже завжди знаходяться у сплячому режимі і на зв'язок виходять тільки періодично. Крім того, сенсорні мережі розгортаються на великих територіях з кількістю вузлів порядку декілька сотень. Це означає, що розробники повинні звернути особливу увагу на мінімізацію споживання енергії, що може бути забезпечено відповідними протоколами передачі даних [2–4].

Усі стандарти моніторингу повинні бути добре захищені від стороннього втручання та працювати на низькій потужності. Стандарти для бездротових додатків, такі як Bluetooth та IEEE 802.11, забезпечують великі швидкості передачі, проте вимагають відповідно високих енергоспоживань, є складними в реалізації та дуже дорогими, тоді як сенсори стандарту ZigBee здатні працювати на низьких потужностях та бути активними менше ніж 1 % часу. Новий вузол такої мережі здатний приєднатися до мережі за 30 мс. Сплячий вузол виходить на зв'язок вже за 15 мс. Усі ці характеристики відповідають вимогам сенсорів для різних медичних додатків, наприклад, датчик вимірювання тиску крові в людини може виходити на зв'язок раз в годину. Проте найактуальнішим є вимірювання електрокардіограми (ЕКГ) у пацієнтів, тому що стаціонарне проведення цієї процедури обмежує їх мобільність. При застосуванні безпровідного датчика на тілі пацієнта він зможе вільно пересуватися територією санаторію або ж перебувати у власному домі, тоді як його дані ЕКГ будуть періодично передаватись на центральний вузол (сервер), де можуть бути переглянуті черговим або лікуючим лікарем.

Тому розроблення мобільних, зокрема сенсорних мереж контролю стану пацієнтів, наприклад їх ЕКГ, є актуальним завданням.

Характеристики ЕКГ. Електрокардіограма – це інструмент для оцінки електричних подій у межах серця. Потенціали серцевих м'язів можна розглядати як джерела напруги, що змушують рухатися кров тілом людини. Ці потенціали можуть бути виміряні за допомогою електродів на тілі людини [1]. Рис. 1 зображає типову ЕКГ, коли електроди розміщені на правій руці та лівій нозі пацієнта.

Перше виявлення хвилі P належить до деполяризації серцевих м'язів. У нормальному стані P-хвиля має різні форми від плоскої до гострої хвилі з амплітудою від 0 до 0,3 мВ. Інтервал P-R є продовженням початку хвилі P до першого компонента комплексу QRS. Наступним проявом є комплекс QRS, що відповідає за деполяризацію шлуночків серця. Фінальним виявленням є хвиля T, яка є результатом реполяризації шлуночків. Реполяризація серцевих м'язів переважно не відображається на ЕКГ, оскільки збігається за часом з QRS комплексом.

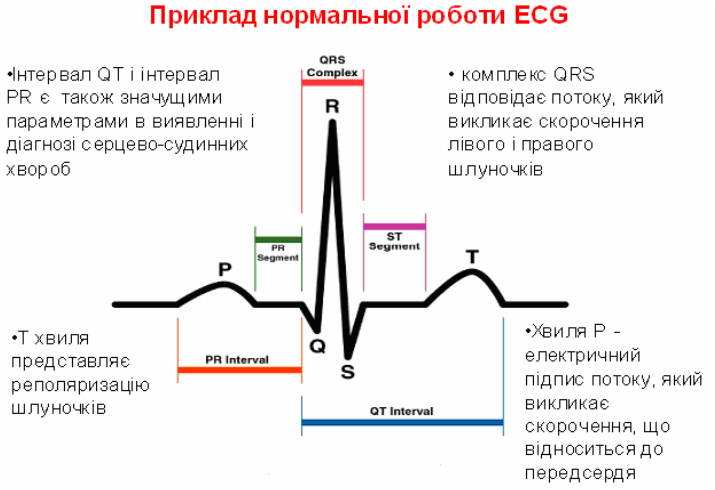


Рис. 1. Типова ЕКГ людини

Алгоритм мобільної передачі ЕКГ

Більшість платформ для вимірювання ЕКГ функціонують такими двома різними способами [2]. У першому режимі вимірюється та на місці аналізується зміна ЕКГ. Якщо якась аритмія серця виявлена, то сигнал тривоги передається на центральний пункт моніторингу за допомогою ZigBee-мережі. У другому режимі кардіограма знімається та безпосередньо передається на центральний пункт, який і приймає рішення про певні відхилення в здоров'ї пацієнта. ZigBee-протокол не підтримує сегментації та реасемблювання даних. Тому усі ці процедури опрацювання ЕКГ виконуються на прикладному рівні системи OSI. Головними функціями більшості платформ є амплітудна модуляція, квантування та алгоритми виявлення основних характеристик електрокардіограми (рис. 2). Типовий сигнал ЕКГ на тілі людини коливається в районі 2 мВ. Цей сигнал пропускається через диференціюючий фільтр та фільтр низьких частот, як зображено на рис. 2, де $E(k)$ – відповідає квантованій кардіограмі. Частоту дискретизації у цьому випадку вибирають 320 Гц.

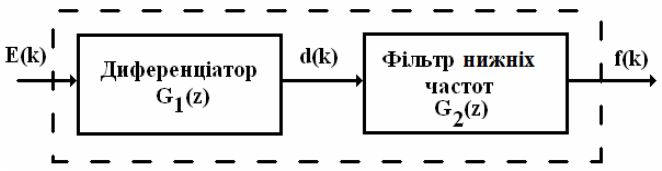


Рис.2. Фільтри для ЕКГ

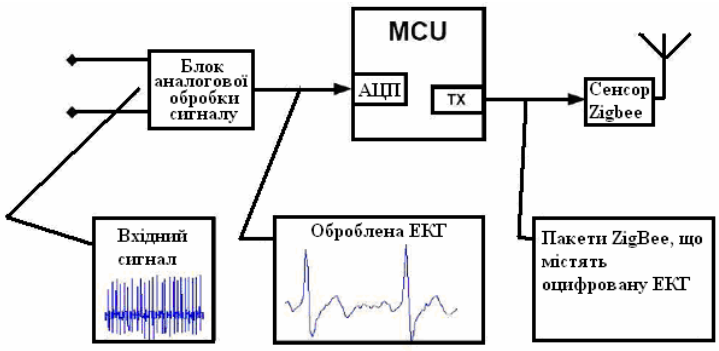


Рис. 2. Блок-схема датчика ЕКГ

Диференціатор має таку характеристику:

$$G_1(z) = 1 - z^{-1},$$

він використовується для виявлення QRS комплексу. $G_2(z)$ є фільтром нижніх частот для зменшення залишкового шуму та шуму квантування. Основною функцією фільтра $G_2(z)$ є максимізація енергії QRS комплексу та виявлення R піку.

Виявлення QRS-піків

Для виявлення піків QRS використовується адаптивний поріг. Внаслідок руху пацієнта форма хвилі ЕКГ сигналу може змінюватись за кожного наступного удару серця. З використанням адаптивного порога ймовірність пропуску QRS-піку зменшується. У запропонованому алгоритмі, за перші п'ять секунд шукається максимальне абсолютне значення відфільтрованих даних ЕКГ – $f(n)$. Позначимо величину цього піку як p_0. Початковий поріг визначається як: $\tau_0 = \alpha p_0$, де α>0. В [1] пропонується вибирати α=0.65.

Нехай p_i – перший локальний пік $f(n)$ після визначення початкового порога. Наступний поріг тоді визначається так:

$$\tau_i = \alpha \tau_{i-1} + (1-\alpha) p_{i-1}.$$

Тривалість інтервалу між піками двох послідовних R-хвиль дає миттєве серцебиття. Їх послідовна зміна показує зміни у серцебитті (рис. 4).

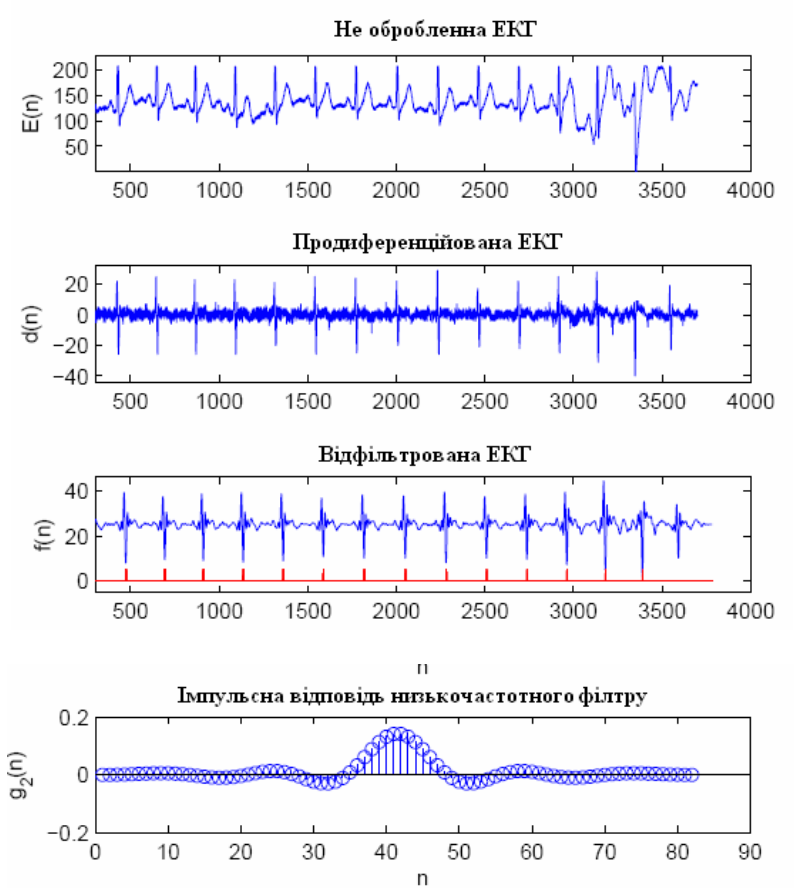


Рис. 4. Послідовність ЕКГ та ЕКГ після детектора піку R

Характеристики пристроїв ZigBee

В основі технології ZigBee/802.15.4 існує три класи пристроїв: FFD-пристрої маршрутизації (*Full Function Device – пристрій з повним комплектом функцій*), пристрої-координатори (*Coordinators — FFD з додатковими ресурсами системи залежно від складності мережі*) і RFD-кінцеві пристрої (*Reduced Function Device – пристрій з обмеженим набором функцій*) [3, 4]. У

кожній локальній мережі ZigBee присутній тільки один координатор. Його основне завдання полягає у встановлені параметрів і створенні мережі, виборі основного радіочастотного каналу, в заданні унікального мережевого ідентифікатора. Тому координатор є найскладнішим з цих трьох типів пристроїв, має великий обсяг пам'яті і підвищене енергоспоживання (як правило, застосовується живлення від мережі змінного струму).

Маршрутизатори використовуються для розширення радіуса дії мережі, тому що здатні виконувати функції ретрансляторів між пристроями, розміщеними далеко один від одного. Маршрутизатори підтримують будь-яку топологію мережі ZigBee, можуть виконувати функції координатора і звертатися до усіх вузлів мережі (FFD, RFD).

Пристрої з обмеженим набором функцій не беруть участі у маршрутизації, не можуть виконувати функцію координатора, звертаються тільки до координатора локальної мережі (FFD-пристрою), підтримують топології типу «кожен з кожним», «зірка», відіграють роль кінцевих вузлів мережі.

На практиці більшість вузлів мережі – RFD-пристрої, а використання FFD-пристроїв і координаторів потрібне для утворення мостів зв'язку і відповідної топології мережі. Як тільки маршрутизатори та інші пристрої під'єднуються до мережі, вони отримують інформацію про неї від координатора або будь-якого іншого існуючого маршрутизатора, вже залученого в мережу, і на основі цієї інформації встановлюють свої операційні параметри відповідно до характеристик мережі. Маршрутизатор ZigBee отримує таблицю мережевих адрес, які він поширює між сполученими з ним кінцевими пристроями. Пристрій FFD використовує деревоподібну скорочену адресацію під час ухвалення рішення про маршрут. Кожен маршрутизатор, на якому дозволено використовувати скорочення, повинен підтримувати таблицю, що містить пари виду DN, де D – адреса призначення і N – адреса наступного пристрою на шляху до призначення. Комбінація маршрутизації на деревоподібному принципі забезпечує гнучкість роботи і надає розробникам вибір оптимального відношення ціна/продуктивність.

Використання топології багатокластерної мережі для збору даних ЕКГ

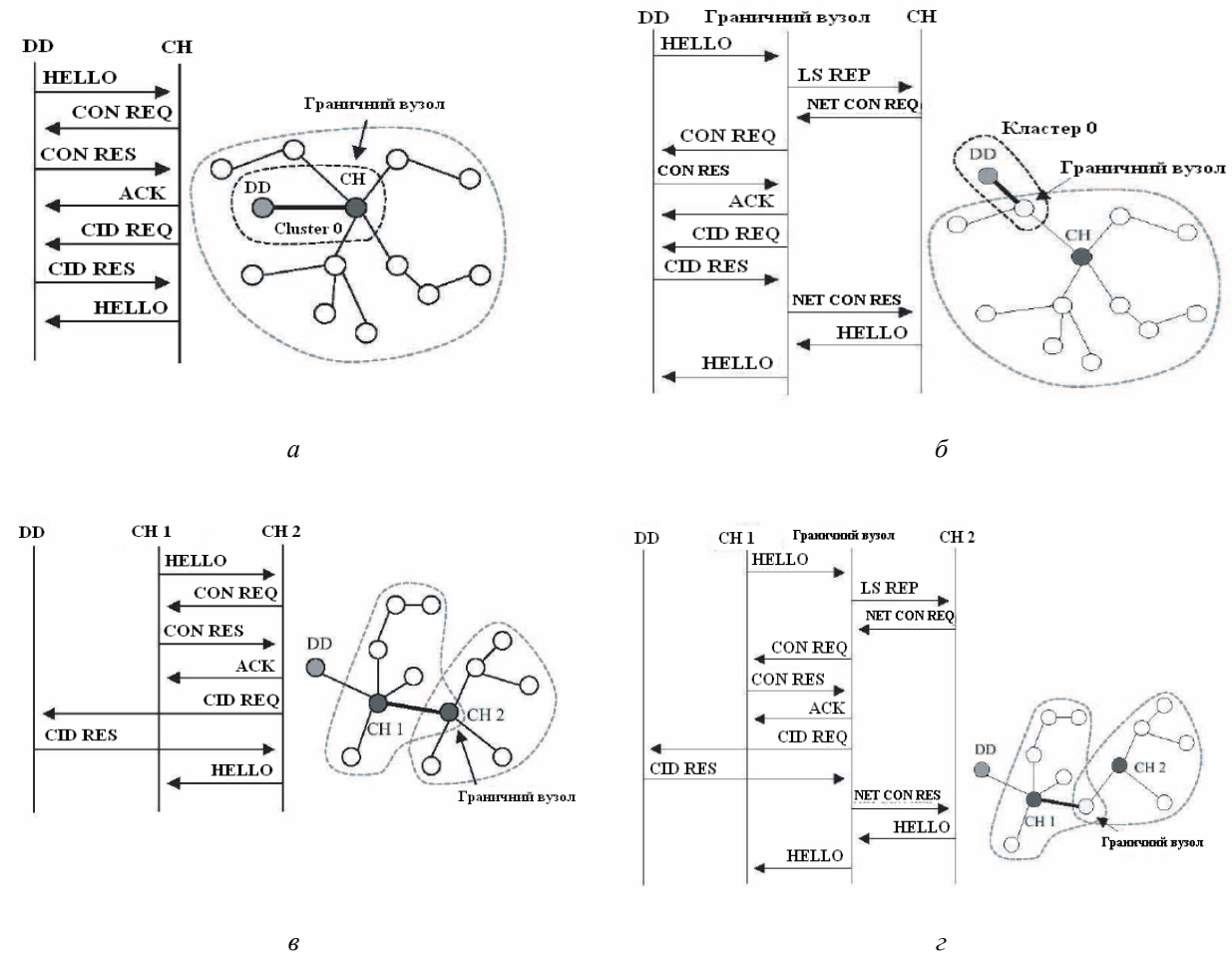
Для розв'язання задачі побудови мереж моніторингу ЕКГ пацієнтів доцільно використовувати багатокластерну мережу. Щоб сформувати цю мережу, необхідно встановити спеціальний помічений вузол (DD). Він потрібний для того, щоб призначити унікальний кластерний ідентифікатор (CID) для мережевого сенсора, що комбінується з вузловим ідентифікатором. Іншою функцією DD є обчислення найкоротшого шляху до кожного кластера та інформування про це інших вузлів у мережі.

Коли DD приєднується до мережі, він розсилає повідомлення HELLO усім сусідам, під час отриманя цього повідомлення сусідній сенсор відправляє у відповідь запит "CONNECTION REQUEST" для приєднання до нульового кластера. Після цього вузол очікуватиме ідентифікатор кластера CID від DD. У цьому випадку CH стане граничним вузлом з двома логічними адресами, одна для ідентифікації його як учасника кластера 0, інша – вершини кластера. Коли CH отримає кластерний ідентифікатор CID, він проінформує учасників свого кластера про це за допомогою повідомлення HELLO. Якщо учасник кластера отримає повідомлення HELLO, то вони додадуть до таблиці сусідів кластерний ідентифікатор 0 та відрапортують про це CH. Вершина кластера вибирає серед членів кластера вузол для того, щоб зробити його граничним вузлом до центрального кластера, та висилає NETWORK CONNECTION REQUEST-повідомлення до граничного вузла про початок встановлення процедури з'єднання з DD. Граничний вузол вишле запит про з'єднання та вступ у нульовий кластер. Після цього він вишле CID REQUEST-повідомлення до DD. Після отримання CID RESPONSE-повідомлення граничний вузол вишле NETWORK CONNECTION RESPONSE-повідомлення, що міститиме новий кластерний ідентифікатор до свого заголовка кластера. Коли CH отримає новий CID, він повідомить про нього членів свого кластера за допомогою повідомлення HELLO.

Кластери, що безпосередньо не межують з нульовим кластером, використовують проміжні ланки для отримання кластерного ідентифікатора.

Усі описані вище процедури отримання кластерного ідентифікатора зображено на рис. 5, *а–г*.

Кожен член кластера повинен знати про центральний кластер, дочірні/нижчі кластери та вузлові ідентифікатори граничних вузлів. DD повинен мати відомості про усю деревоподібну структуру кластерів. Вузли в кластері та CH відсилають інформацію про свої безпосередні зв'язки до DD. Згодом ця інформація може бути використана для розрахунку оптимізації топології мережі. Отже, DD може розсилати "TOPOLOGY UPDATE"-повідомлення для інформування про сучасні маршрути від DD до інших кластерів.



а *б*

в *г*

Рис. 5. Варіанти встановлення кластерного ідентифікатора

Можливе існування резервного DD для підтримки мережі в момент падіння DD. Міжкластерна комунікація, що зображена на рис. 6, реалізується за допомогою маршрутизації [5]. Граничні вузли відіграють роль раутерів між двома кластерами. Коли граничний вузол отримає пакет, він перевірить адрес призначення, згодом відправить до наступного граничного вузла прилеглого кластера.

Лише DD може вислати повідомлення до усіх вузлів в мережі. Повідомлення буде розіслане деревоподібною структурою кластерів. Граничні вузли відішлють це повідомлення від батьківських до дочірних кластерів.

Якщо відбулося об'єднання згідно з правилами вже існуючої мережі, координатор примикаючої локальної мережі переводиться в ранг маршрутизатора і передає усю інформацію про локальну мережу координаторові існуючої мережі (рис. 6). З сигнального пакета синхронізації від координатора новоутворений маршрутизатор отримає необхідну інформацію про тимчасові параметри мережі для виявлення подальших сигнальних пакетів. Приклад зміни топології показано на рис. 7.

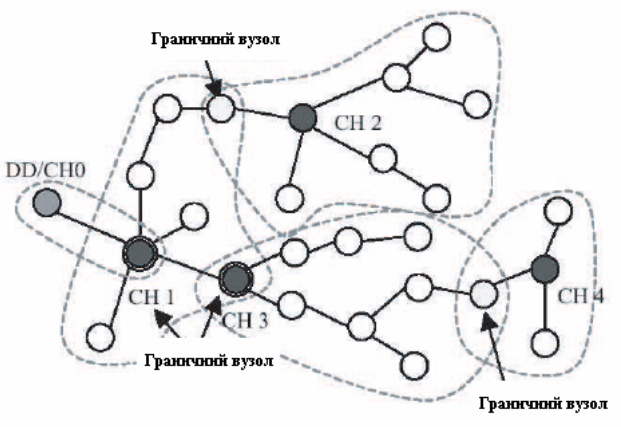


Рис. 6. Багатокластерна мережа та граничні вузли

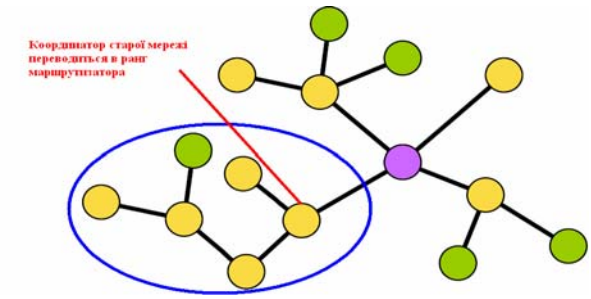


Рис. 7. Об'єднання двох мереж ZigBee

Отже, для практичної реалізації сенсорної мережі на основі стандарту ZigBee найоптимальнішою є кластерна топологія, оскільки вона дає змогу створити ієрархічну структуру вузлів (координатор – маршрутизатор – кінцевий пристрій).

Аналіз мобільності вузлів. Однією з характеристик сенсорних мереж є динамічна топологія. Це часто призводить до обривів зв'язку та анулювання певних маршрутів. Оскільки зв'язки у цих мережах характеризуються різними пропускними здатностями та ємністю, то можливе переповнення буферів. Також, оскільки робота вузлів залежить від акумуляторної батареї, то енергозаощадження є важливою функцією. Але масштабованістю *ad hoc* мережі не можна нехтувати, оскільки деякі мережі можуть бути доволі великими. Усі ці важливі характеристики в певний спосіб впливають на наявність маршруту у потрібний час. Беручи це все до уваги, протокол маршрутизації повинен проводити ефективну маршрутизацію.

Основні характеристики протоколів маршрутизації

Переважно при виборі протоколу потрібно відповісти на питання: Протокол використовується для одно- чи багатоканальної системи? Для одноканальної системи деякі протоколи використовують передачу маяка для виявлення порушень зв'язків або ж застосовують вищі рівні, тоді як інші проводять аналіз переданого трафіка.

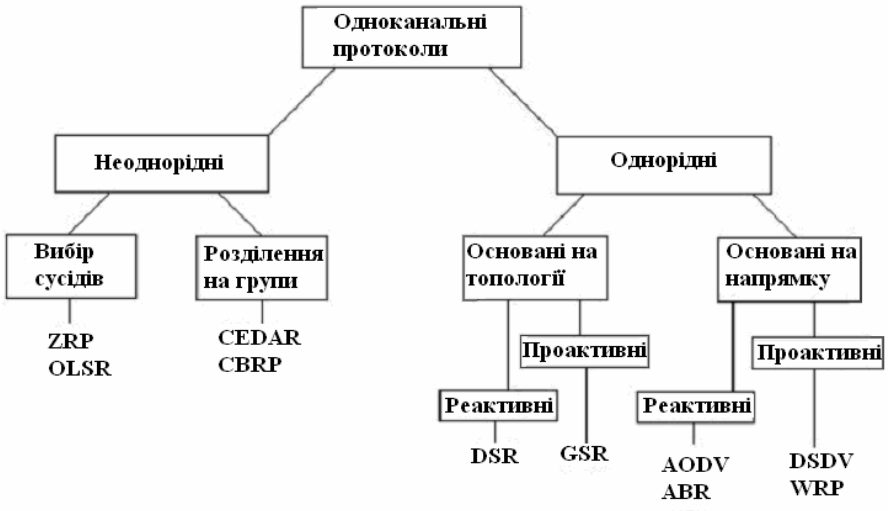


Рис. 8. Поділ протоколів в сенсорних мережах

Багатоканальні протоколи використовують також нижчі рівні та комбінують маршрути і доступ до каналу. Для спрощення опису приймемо, що у нашій мережі застосовуватимуться лише одноканальні протоколи.

Вибір протоколів. Оскільки протоколів маршрутизації існує багато, то з класифікації, зображеної на рис. 8, вибрано гібридний кластерний протокол маршрутизації стандарту ZigBee (HCR).

Цей протокол зменшує затримки у маршруті та службові заголовки пакета, що означає керованість контрольного трафіку в мережі. Оскільки кластерна топологія організована на двоярусній структурі, то протокол HCR розділяє маршрутизацію на дві частини: міжкластерну маршрутизацію та маршрутизацію всередині кластера. Міжкластерна маршрутизація знаходиться на вищому рівні, оскільки передача відбувається від кластера до кластера. Маршрутизація всередині кластера є на нижчому рівні, оскільки передача відбувається лише від вузла до вузла. Подібно до інших протоколів маршрутизації HCR має дві основні функції: відкриття та обслуговування маршруту [6].

Процедура відкриття маршруту. Коли джерельний вузол має пакети для передачі у певному напрямі, він перевіряє власну таблицю маршрутизації для того, чи немає там активного маршруту до вузла призначення. Якщо немає, то вузол повинен провести процедуру відкриття маршруту для того, щоб дізнатися маршрут до вузла призначення. В HCR відкриття маршруту складається з двох частин: міжкластерне відкриття маршруту та відкриття маршруту всередині кластера. Міжкластерне відкриття маршруту розпочинається з надсилання запиту листа кластерів (CLREQ) до властого заголовка кластерів. Після одержання CLREQ, CH відішле відповідь на запит CLREP до ініціатора. Після перевірки вузлом відповіді він проведе оновлення власної таблиці маршрутизації. Якщо вузол не одержить відповідь на запит, то він повторюватиме цю процедуру ще MAX_CLREQ разів. Відкриття маршруту всередині кластера проходить у випадку, коли вузлу необхідно передати інформацію до іншого вузла, що знаходиться у тому самому кластері. Коли вузол одержав запит RREQ, він перевіряє, чи зможе він відповісти на цей запит. Можливі два варіанти відповіді: вузол зазначений у запиті є вузлом, що прийняв повідомлення, або ж цей вузол знаходиться десь дальше у мережі; вузол, що одержав це повідомлення, перевірить, чи немає в його таблиці маршрутизації маршруту до цього вузла. Якщо відбулася одна з описаних подій, то вузол відправить відповідь RREP. RREQ також широкомовно можуть ретранслюватися.

Процедура передачі даних. Коли джерельний вузол одержить відповідь на запит про маршрут, він розмістить лист кластерів у заголовку пакетів. З цього часу актуальні пакети будуть скеровані або до шлюзових вузлів, або до вузла призначення всередині власного кластера. Коли шлюзовий вузол одержить пакет, він повинен перескерувати цей пакет до наступного кластера згідно з листом кластерів. Так, пакет передаватиметься від кластера до кластера до того часу, поки він не досягне кластера з вузлом призначення (рис. 9).

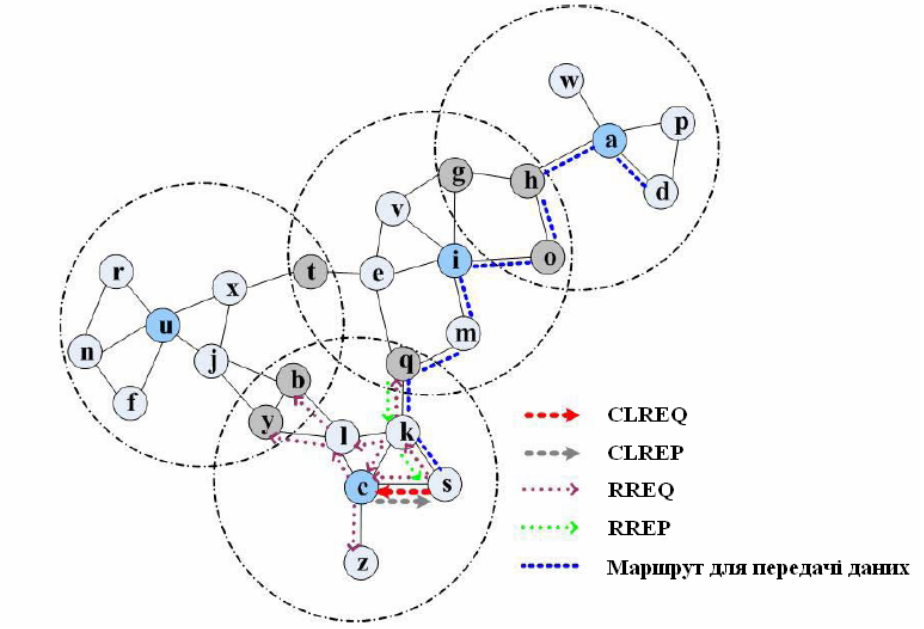


Рис. 9. Приклад встановлення маршруту та передачі даних

Обслуговування маршруту. Кластерна топологія здатна змінюватися (розрив певних зв'язків) у зв'язку з мобільністю вузлів. Тому інформація про мережу або в загальній таблиці маршрутизації, або в пакетному заголовку може втратити свою актуальність. Обслуговування маршрутів – це певний механізм, завдяки якому пакети все таки одержуються вузлом призначення, незважаючи на зміни у топології. В HCR запропонована схема, яка називається глобальним відновленням для збереження пакетів та для оновлення інформації про маршрути. Коли заголовок кластера виявить помилку в маршруті, він створить нову кластерну таблицю через метод місця призначення. Повідомлення – таблиця помилок в кластерах CLERR, що містить нову кластерну таблицю, буде безпосередньо передана до ініціатора з'єднання. Коли джерельний вузол одержить CLERR, він побудує повний новий кластерний лист, використовуючи інформацію з одержаного повідомлення. У прикладі глобального відновлення, зображеного на рис. 10, вузол S передає дані до вузла D через лист кластерів {A,I,C}. Проте кластери I та C стають відокремленими завдяки мобільності певного вузла. Тоді заголовок кластера I одержить RREQ про маршрут до кластера C від вузла H. Тоді повідомлення CLERR буде безпосередньо передано вузлу H від вузла I. Завдяки одержаному CLERR вузол H побудує новий кластерний лист {A, I, U, C}. Після цього вузол S одержить CLERR-повідомлення, завдяки чому змінить власний кластерний лист для подальшої передачі повідомлень до вузла D (рис. 10).

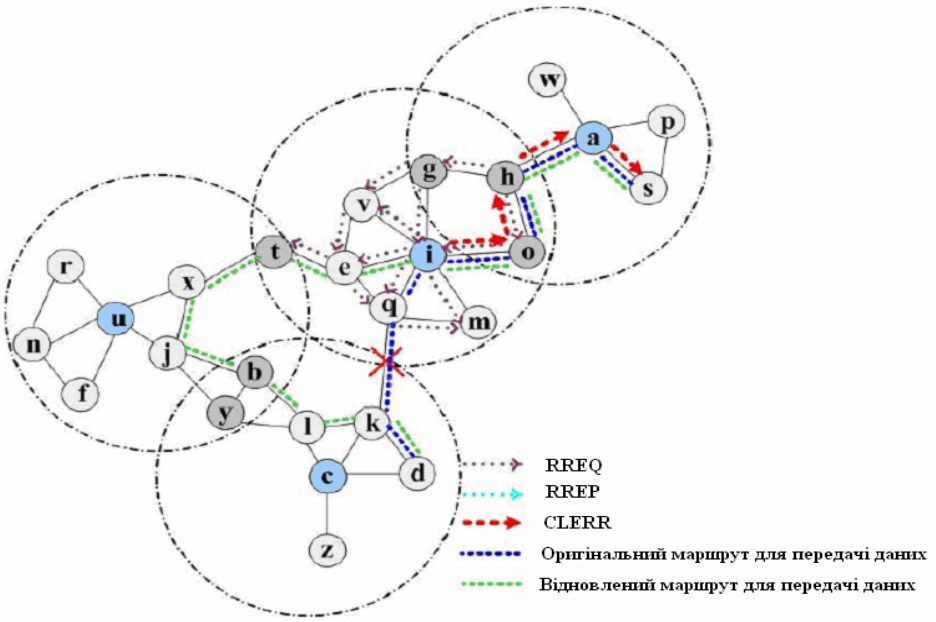


Рис. 10. Приклад глобального віднoвлення маршруту

Аналіз параметрів сенсорної мережі

Симуляція та аналіз сенсорної мережі проведені за допомогою мережевого стимулятора NS-2. На початку дослідження вважалось, що існує однакова щільність вузлів. Усі вузли мають мінімальний радіус передачі 50 м та випадково розміщені на вибраній території. Також ключовими параметрами мережі, що задаються, є: кластерний радіус=2, INTRA_CB_INTERVAL = 5 с, та INTER_CB_INTERVAL = 10 с. До даних, які потрібно розрахувати, належать: розмір пакетного заголовка, співвідношення пакетів, що передані до тих, які прийняті, та середній час затримки під час передачі з кінця в кінець. Для симуляції були вибрані описані вище протоколи: AODV, DSR, CBRP та HCR.

Мета дослідження – порівняти роботу вибраних протоколів та виявити їх реакцію на зміни в мережі та зміни руху контрольного трафіка. У кінці проведених експериментів було одержано результати, зображені на рис. 11.

На рис. 11 зображено залежність розміру пакетного заголовка, показано, що він збільшується при зростанні розмірів мережі для усіх протоколів. У HCR заголовок є доволі малим, навіть у випадку, коли

кількість вузлів є більшою від 150, що частково пояснюється кластерною схемою обслуговування вузлів та схемою маршрутизації пакетів. Розмір пакетного заголовка при міжкластерному та внутрікластерному відкритті маршруту обмежується у межах кластера замість цілої мережі. Окрім того, інформація встановлення маршруту всередині кластера згодом може бути використана під час міжкластерної маршрутизації. До того ж використання глобального ремонту також зменшує розмір пакетного заголовка порівняно з локальним ремонтом у трьох інших протоколах.

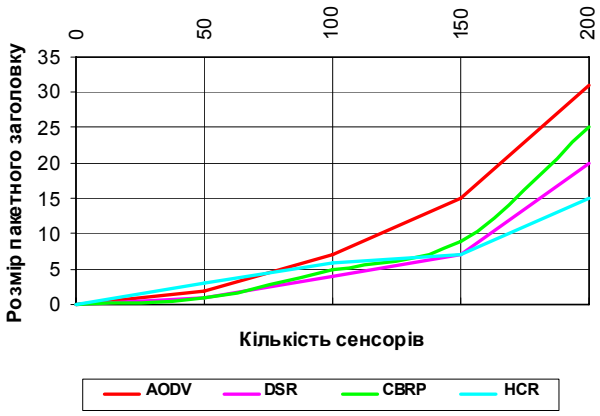


Рис. 11. Залежність розміру пакетного заголовка від кількості вузлів

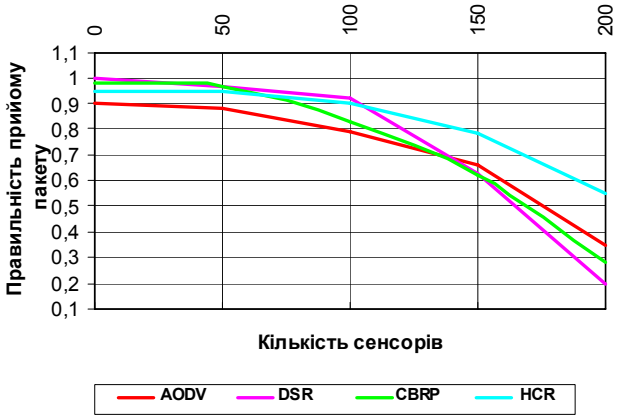


Рис. 12. Відсоток правильно прийнятих пакетів

Як показано на рис. 12, правильність прийому пакетів зменшується за збільшеня розмірів мережі для усіх чотирьох протоколів. Значення HCR приблизно дорівнює значення протоколів AODV та CBRP. Проте, коли розміри мережі стають більшими, перевага HCR стає очевидною завдяки меншому порівняно з іншими протоколами пакетному заголовку.

Рис. 13 показує середній час затримки пакета в мережі для кожного з вибраних протоколів. За збільшення розмірів мережі зростає час затримки для усіх чотирьох протоколів. Однак HCR функціонує краще за інших за великих розмірів мережі. З вищезгаданого бачимо, що за великих розмірів мережі пакетний заголовок в HCR є порівняно малим, що забезпечує швидше звільнення буферів вузлів, а відповідно і зменшення затримок у мережі.

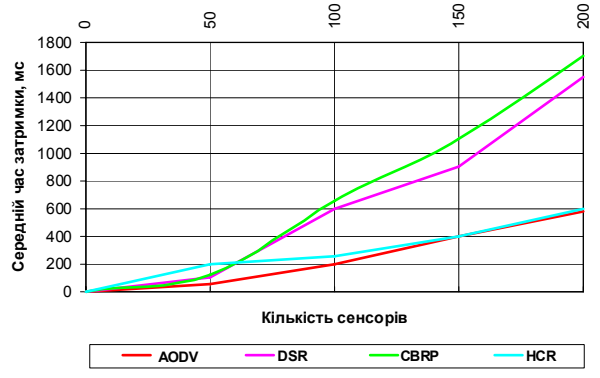


Рис. 13. Відношення середнього часу затримки залежно від кількості вузлів

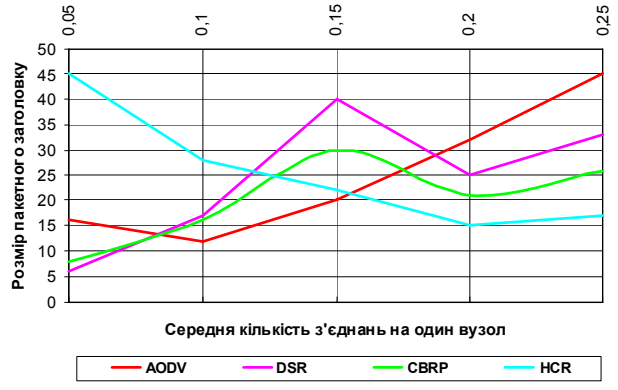


Рис. 14. Залежність розміру пакетного заголовка залежно від кількості з'єднань в мережі

Аналіз завантаження мережі. На рис. 15, 16 зображені відношення для метрик залежно від завантаження мережі (тобто від реальної кількості з'єднань між вузлами) за стабільної кількості вузлів. Зміна кількості з'єднань між вузлами лежить у межах від 0,05 до 0,25. Як показано на рис. 14, пакетний заголовок в HCR зменшується порівняно з іншими протоколами за зростання кількості з'єднань в мережі.

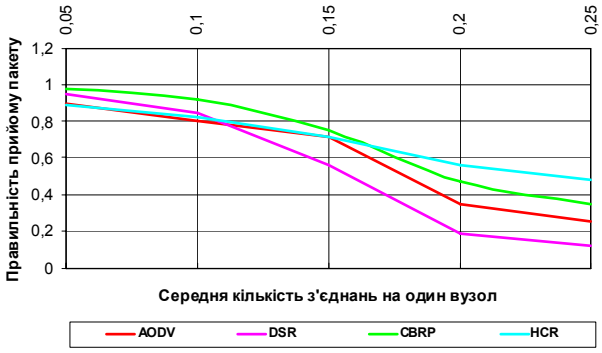


Рис. 15. Відношення правильно прийнятих пакетів до кількості з'єднань на один вузол

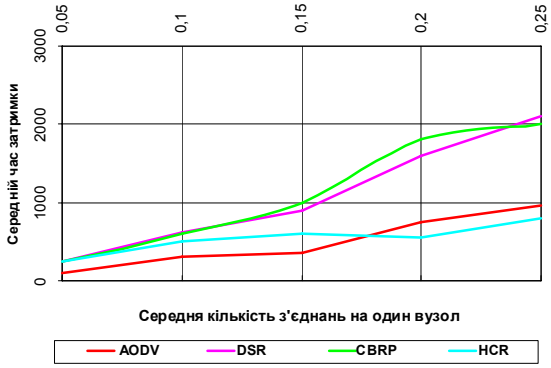


Рис. 16. Залежність часу затримки у мережі від кількості з'єднань на вузол

Це зменшення пакетного заголовка в HCR є тому, що він має власні схеми обслуговування та відкриття маршруту. Як описано вище, заголовок кластерного обслуговування маршруту є фіксованою частиною заголовка з маршрутизації. Чим більше потрібно з'єднань, тим частка заголовка обслуговування в загальному заголовку стає порівняно меншою. Тому зменшення пакетного заголовка сприятиме швидшому сприйняттю пакета та зменшенню середнього часу затримки. Збільшення часу затримки для трьох інших протоколів пов'язане з лавиноподібним розмноженням запитів пошуку нових маршрутів та збільшенням заголовка обслуговування маршрутів за збільшення їх кількості.

Висновки

Проведений аналіз показує, що найкращим протоколом для реалізації проекту мобільного моніторингу ЕКГ є протокол HCR. Для маршрутизації кластери у цьому протоколі складаються із заголовків кластерів, шлюзових та кінцевих вузлів. Заголовок кластера відповідає за підтримку локального членства вузлів свого кластера та за знання глобальної кластерної топології. Міжкластерну інформацію одержують за допомогою проактивного методу, тоді як інформацію всередині кластера одержують за допомогою методу "на вимогу". Проведені симуляції та теоретичний аналіз показують, що HCR має кращу масштабованість та пристосованість до певних умов, ніж інші відомі протоколи маршрутизації.

1. Дабровски А., Дабровски Б., Пиотрович Р. Суточное мониторирование ЭКГ. – М.: Медпрактика, 2000. – 208 с. 2. http://www.autobuilding.ru/articles.html. 3. Callaway E.H. Wireless Sensor Networks: Architectures and Protocols. – New York: CRC Press LLC, 2004. 350 p. 4. Rishi Pidva "Security in Wireless Sensor Networks" (March 3 2003 http://www.cs.wmich.edu/wsn/doc/spins/Pidva_SPINS.pdf). 5. Mengke Li "Secure Routing Protocols in Wireless Sensor Networks" (November 2004 http://cse.unl.edu/~hcheng/courses/csce990/mli-cse990F2004.ppt). 6. Куприянов А.Е. Стек протоколов защищенной вероятностной маршрутизации в беспроводных сенсорных сетях // 6–12. Kupriyanov.doc.