Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)

Кафедра Інформаційно-мережної інженерії
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)
Дослідження та вибір протоколів маршрутизації бездротових сенсорно-актуаторних мереж
(тема)

Виконав:
Здобувач другого року навчання,
групи ІМІм-24-1
Марадудін Ілля Олексійович
(власне ім'я, прізвище)
Спеціальність 172 Електронні комунікації та радіотехніка
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Інформаційно-мережна інженерія
(повна назва освітньої програми)

Керівник *доц. Юлія Скорик*
(посада, власне ім'я, прізвище)

Допускається до захисту

Завідувач кафедри _____ _____ *Микола Москалець*
(підпис) (власне ім'я, прізвище)

2025 р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій

Кафедра Інформаційно-мережної інженерії

Рівень вищої освіти другий (магістерський)

Спеціальність 172 Електронні комунікації та радіотехніка
(код і повна назва)

Тип програми Освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Інформаційно-мережна інженерія
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)
«_24_»____10_____ 2025___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Марадудіну Іллі Олексійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження та вибір протоколів маршрутизації бездротових сенсорно-актуаторних мереж

затверджена наказом університету від _24___ ___10_____2025 р. № 959Ст___

2. Термін подання здобувачем роботи до екзаменаційної комісії _22__ __12_____ 2025 р.

3. Вихідні дані до роботи *Провести аналіз протоколів бездротових сенсорно-актуаторних мереж. Проаналізувати метод аналізу ієрархій і метод експертного оцінювання. Застосувати ці методи для вибору переважного варіанта протоколу маршрутизації який використовується в бездротових сенсорно-актуаторних мережах з урахування сукупності показників якості*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Вступ

1. Огляд і аналіз протоколів маршрутизації

2. Огляд методів аналізу протоколів

3. Метод аналіза ієрархій і метод експертного оцінювання для вибору переважного протоколу маршрутизації бездротових сенсорно-актуаторних мереж

Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____
Слайди у форматі Power Point *(назва, мета і актуальність кваліфікаційної роботи, протоколи маршрутизації, метод аналізу ієрархій і метод експертного оцінювання, практичне застосування методів на прикладі вибору протоколів бездротових сенсорно-актуаторних мереж , та ін.)*

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата
Основна частина	доц. Скорик Ю.В.		20.12.2025

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / термін виконання етапів роботи	Примітка
1	Ознайомлення із завданням. Уточнення ТЗ	24.10-26.10.2025	виконано
2	Підбір літератури за темою роботи	27.10-01.11.2025	виконано
3	Виконання розділу 1	02.11-17.11.2025	виконано
4	Виконання розділу 2	18.11-22.11.2025	виконано
5	Виконання розділу 3	23.11-09.12.2025	виконано
6	Оформлення презентаційного матеріалу	10.12-19.12.2025	виконано
7	Підготовка до захисту у ЕК	20.12-22.12.2025	виконано

Дата видачі завдання __24___ _____10_____2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ __*доц. Юлія Скорик*_____
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 59 стор. формату А4, 7 рис., 14 табл., 19 посилань.

Мета роботи – провести аналіз методу вибору переважного протоколу маршрутизації, а також вибрати переважний протокол маршрутизації, який використовується в бездротових сенсорно-актуаторних мережах.

Розглянуто процес вибору ефективного протоколу маршрутизації для застосування в польових сенсорних мережах з локалізацією елементів методом аналізу ієрархій. В результаті порівняльного аналізу обраний енергоефективний протокол маршрутизації на основі розташування вузлів бездротових сенсорно-актуаторних мереж.

СЕНСОРНА МЕРЕЖА, МАРШРУТИЗАЦІЯ, КРИТЕРІЇ ВИБОРУ, ЕНЕРГОЕФЕКТИВНІСТЬ, МЕТОД АНАЛІЗУ ІЄРАРХІЙ, ЕКСПЕРТ.

ABSTRACT

Explanatory note: 59 pp. format A4, 7 Fig., 19 reference, 14 tab.

Object of work – analyze the method of choosing a preferred routing protocol, and choose the preferred routing protocol used in wireless sensory actuator networks.

The process of choosing an efficient routing protocol for use in field sensor networks with localization of elements by the method of analysis of hierarchies is considered. As a result of the comparative analysis, the selected energy efficient routing protocol is based on the location of the nodes of the wireless sensor-actuator networks.

SENSOR NETWORK, ROUTE, SELECTION CRITERIA, ENERGY EFFICIENCY, THE ANALYTIC HIERARCHY PROCESS, EXPERT.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

GAF – Geographic Adaptive Fidelity;

GEAR – Geographicand Energy – Aware Routing;

LEACH – Low Energy Adaptive Clustering Hierarchy;

QoS – Quality Of Service;

PEGASIS – Power-Efficient Gathering in Sensor Information Systems;

SAR – Sequential Assignment Routing;

SNFG – StatelessGeographic Non-Deterministic Forwarding;

SOP – Self-Organizing Protocol;

SPEED – Stateless protocol for real-time communication;

SPIN – Sensor Protocols for Information via Negotiation;

TDMA – Time division multiple access;

TEEN – Threshold Sensitive Energy Efficient Sensor Network Protocol;

БС – базова станція;

БСАМ – бездротові сенсорно-актуаторні мережі;

МАІ – метод аналізу ієрархії.

ВСТУП

За останній період інтенсивний розвиток бездротових сенсорно-актуаторних мереж (БСАМ) зумовив появу значної кількості протоколів, алгоритмів та спеціалізованих специфікацій, орієнтованих на розв’язання різноманітних задач. Серед них – ефективний збір даних, визначення місцезнаходження окремих елементів мережі, задачі маршрутизації, яким присвячена дана робота, а також багато інших. Така різноманітність рішень підвищила потребу у використанні методів, що дозволяють обґрунтовано обирати найбільш ефективні протоколи для конкретних умов застосування. Одним із таких підходів є метод аналізу ієрархій.

БСАМ широко застосовуються для практичних задач розподіленого збору інформації про контрольовані параметри в системах моніторингу та управління. Подібні мережі, як правило, є гомогенними, самоорганізованими, одноранговими, мають комірчасту топологію, а їх вузли оснащені автономними джерелами живлення та здатні передавати інформацію шляхом ретрансляції. Використання батарей як джерела живлення накладає суттєві обмеження на енергоспоживання всіх алгоритмів, що функціонують у сенсорних мережах. У зв’язку з цим для БСАМ особливо актуальними є такі задачі маршрутизації: задача визначення оптимальних маршрутів і задача маршрутизації з метою максимального подовження часу функціонування мережі [1].

З урахуванням зазначених критеріїв у даній атестаційній роботі досліджується використання методу аналізу ієрархій разом із методом експертних оцінок для вибору протоколів маршрутизації в польовій БСАМ із відомим розташуванням елементів мережі.

1 ОГЛЯД І АНАЛІЗ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ

Розглянемо види алгоритмів, які найбільше використовуються для додатків БСАМ:

– Розподілені алгоритми. Зв’язок забезпечується через процес обміну інформацією між вузлами.

– Централізовані алгоритми. Засновані на принципі, за яким один вузол має повну інформацію про всю мережу. Такі алгоритми застосовуються вкрай рідко через значні енергетичні витрати, пов’язані з передачею даних про стан мережі до головного вузла.

– Алгоритми, що базуються на місцезнаходженні. Передбачають використання вузлами даних про найближче оточення для локальної маршрутизації.

Парадигма алгоритму маршрутизації є ключовим чинником під час вибору протоколу маршрутизації для конкретної мережі. У разі використання алгоритмів, орієнтованих на обмежену область, необхідно забезпечити оптимізацію зв’язку між сусідніми вузлами. Для централізованих алгоритмів перевагою є передавання великої кількості повідомлень виключно до центрального вузла. Застосування розподілених алгоритмів вимагає надійного та ефективного зв’язку між будь-якими парами вузлів. Водночас алгоритми, засновані на визначенні розташування, ефективність яких досягається завдяки знанню географічних координат (наприклад, з використанням GPS), призводять до подорожчання рішення [1].

1.1 Протокол SPIN

SPIN розшифровується як Sensor Protocol for Information via Negotiation (Сенсорний протокол для передавання інформації шляхом узгодження). Існує сімейство протоколів, відомих під назвою SPIN, які мають різні варіанти та

функціональні можливості. Ці протоколи розроблені для розв'язання проблем, пов'язаних із поширенням інформації та даних.

SPIN використовує три типи повідомлень: ADV, REQ та DATA. Повідомлення ADV транслюється вузлом, який володіє даними, і інформує про тип даних, що містяться в повідомленні. Зацікавлені вузли, які отримали повідомлення ADV, надсилають повідомлення REQ із запитом на отримання даних. Вузол, що має необхідні дані, передає їх зацікавленим вузлам. Після отримання даних вузли надсилають повідомлення ADV, і процес продовжується (рис. 1.1).

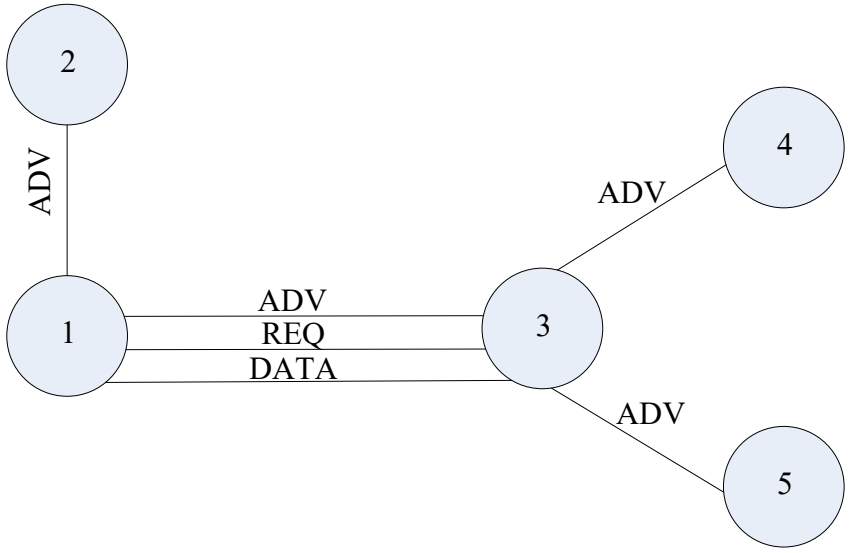

Рисунок 1.1 – Пересилання повідомлень за допомогою SPIN

Вузол 1 надсилає повідомлення ADV всім своїм сусідам, 2 і 3. Вузол 3 запитує дані за допомогою повідомлення REQ, на що вузол 1 відправляє дані за допомогою повідомлення DATA вузлу 3. Після отримання даних вузол 3 відправляє повідомлення ADV своїм сусідам 4 і 5 і процес триває. Він не надсилає дані вузлу 1, тому що вузол 3 знає, що отримав дані від вузла 1.

Дані описуються в пакеті ADV за допомогою високорівневих дескрипторів даних, які є досить хорошими для ідентифікації даних. Ці високорівневі дескриптори даних називаються метаданими. Метадані двох різних даних мають

бути різними, а метадані двох схожих даних схожими. Використання метаданих запобігає розповсюдженню фактичних даних по мережі. Фактичні дані можуть бути надані лише тим вузлам, яким вони потрібні. Цей протокол також робить вузли більш інтелектуальними: кожен вузол матиме менеджер ресурсів, який інформуватиме кожен вузол про кількість ресурсів, що залишилися. Відповідно, вузол може прийняти рішення про те, чи може він виступати як вузл пересилки чи ні [2].

1.2 Протокол Direcied Diffusion

Direcied Diffusion перекладається як Спрямована дифузія. Розглянемо докладніше як працює цей протокол. Вузли, які запитують інформацію, називаються приймачами (sinks), а ті, що генерують інформацію – джерелами (sources). Записи, які вказують на бажання отримати певні типи інформації, називаються інтересами (interests). Інтереси поширюються через мережу, шукаючи вузли з відповідними записами подій. Ключовим моментом спрямованої дифузії є припущення, що інтереси є стійкими – тобто, якщо джерело має інформацію, релевантну приймача, то приймач буде зацікавлений у повторних вимірах від цього джерела протягом деякого періоду часу. Типовий запис інтересу містить поле атрибута інтервалу, що вказує частоту, з якою приймач бажає отримувати інформацію про об'єкти, які відповідають іншим атрибутам запису. Ця довговічність комунікаційних шаблонів дозволяє протоколам спрямованої дифузії вивчати, які шляхи є добрими між джерелами та приймачами, та амортизувати витрати на пошук цих шляхів протягом періоду їх використання (період дії інтересу закодований у його атрибуті тривалості).

Приймачі генерують завдання запиту інформації, чи інтереси, які поширюються сенсорної мережі. Всі вузли відстежують запити на отримання інформації, які вони бачили, але не їх вихідні приймачі. Кожен вузол підтримує кеш запитів на отримання інформації, що містить запис для кожного окремого запиту, який бачив вузол і термін дії якого ще не закінчився; вузол знає тільки, від

якого сусіда надійшов цей запит. Кожен вузол, у свою чергу, може вибрати пересилання запиту деяким чи всім своїм сусідам, тощо. Важливим компонентом спрямованої дифузії є використання градієнтів, пов'язаних з кожним записом у кеші запитів на отримання інформації, які використовуються для направлення та управління потоком інформації назад до приймача, як ми побачимо далі. Оскільки передбачається, що мережа не є ідеально стійкою, періодично кожен приймач повторно транслює повідомлення про запит на отримання інформації. Монотонно зростаючий атрибут тимчасової мітки в кожному записі про запит на отримання інформації використовується для розрізнення цих повторних трансляцій від попередніх версій [3,4].

Градієнт зазвичай визначається частотою, з якою приймач запитує повторні дані про об'єкті, що його цікавить, як згадувалося раніше, і вказує бажану частоту оновлень і сусіда (напрямок), якому повинна бути відправлена ця інформація. Елегантним аспектом спрямованої дифузії є спосіб маніпулювання градієнтами для посилення ефективних шляхів доставки інформації та відключення неефективних. Слід зазначити, що при дифузії інтересів цілком можливо створити два сусідні вузли з градієнтами, спрямованими один до одного, для того самого інтересу. Ця множинність градієнтів не створює стійких петель доставки даних, як ми побачимо, але дозволяє швидко відновлювати шляхи доставки інформації при збоях вузлів або зв'язків.

Як працює направлена дифузія можна подивитись на рис. 1.2.

Припустимо, приймач зацікавлений у виявленні об'єкта у певній невеликій області, що містить один сенсорний вузол. Оскільки маршрут до цієї області невідомий приймачеві, початковий інтерес буде поширюватися по всій мережі. З цієї причини початкова запитувана швидкість передачі даних встановлюється на штучно низьке значення, щоб уникнути надлишкового трафіку кількома зворотними шляхами. Тепер поширення інтересу походить від приймача, поки не буде досягнуто джерело з виявленими об'єктами в області, що цікавить (рис. 1.2). Коли знайдено відповідний запис події, джерело обчислює максимальну швидкість вихідних подій серед усіх своїх градієнтів цього інтересу. Потім вузол

джерела доручає своїй сенсорній підсистемі генерувати вибірки подій з цією максимальною швидкістю передачі і відправляє запис події всім своїм сусідам, котрим має градієнт цієї події. Він продовжує робити це кожному сусідові з відповідною частотою, доки інтерес із боку цього сусіда не зникне.

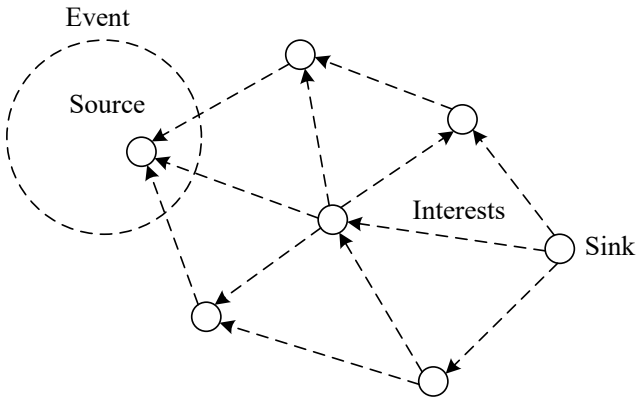

Рисунок 1.2 – Алгоритм спрямованої дифузії поширює інтереси від джерела до тих пір, поки не буде досягнуто відповідне джерело інформації

Вузол, який отримує запис події від своїх сусідів, перевіряє наявність відповідних інтересів у своєму кеші. Якщо їх немає, запис відкидається. Кожен вузол також підтримує кеш даних, у якому записуються недавно отримані записи подій та інші елементи даних. Поточний запис події також відкидається, якщо вона присутня в цьому кеші даних (що вказує на те, що та ж інформація вже надійшла іншим шляхом), запобігаючи таким чином зациклювання пересилання даних. В іншому випадку запис події додається в кеш і також надсилається відповідним сусіднім вузлам, як зазначено відповідними записами в кеші інтересів. Таким чином, запис події поширюється назад до приймача, що запитує. Слід зазначити, що як поширення інтересів, і поширення даних здійснюється виключно локальними операціями, і джерело і приймач ніколи не знають одне про одного. Цей опосередкований спосіб поширення та взаємодії інтересів і даних дозволяє спрямованої дифузії швидко адаптуватися до змін топології мережі, до явищ, що переміщуються по полю датчиків, і так далі.

У наданому прикладі записи подій від вихідного вузла почнуть надходити назад до приймача кількома маршрутами. Це означає, що в кінцевому підсумку приймач може отримувати одні й ті самі дані від кількох сусідів, хоч і тільки з спочатку запрошеною низькою частотою подій (рис. 1.3). На цьому етапі приймач може вибрати посилення певних градієнтів та ослаблення чи усунення інших. Наприклад, перший сусід, який повідомив приймачеві відповідні дані, швидше за все, перебуватиме на шляху з мінімальною затримкою до джерела. Приймач може посилити цей шлях, повторно надіславши цьому сусідові той самий запит, але з більш високою частотою подій.

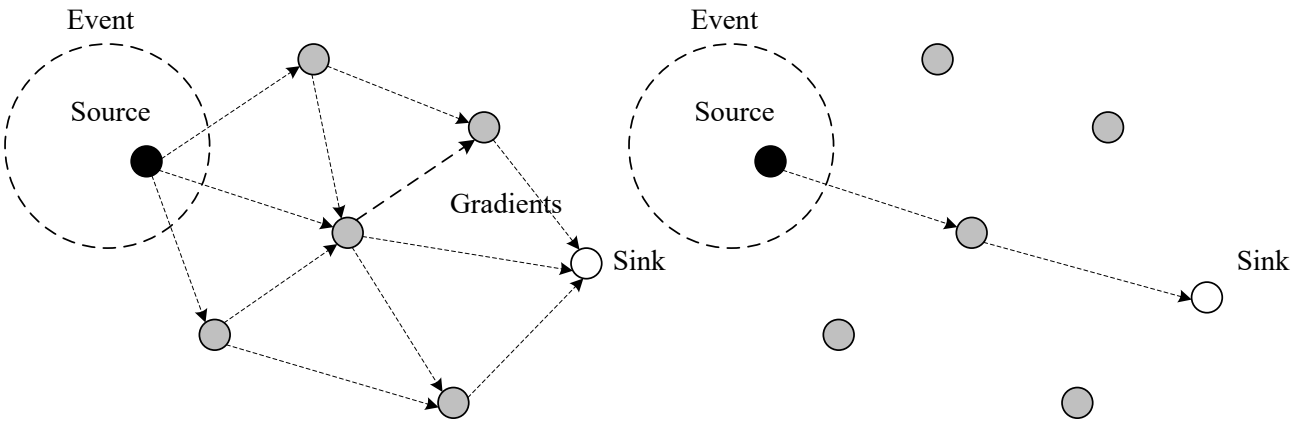

Рисунок 1.3 – Спрямована дифузія створює градієнти передачі інформації від джерела до приймача (ліворуч), що призводить до появи безлічі шляхів передачі. Підкріплення перенаправляє більшу частину інформації оптимальним шляхом (праворуч)

Вузол, який отримав посилений запит, у свою чергу, повинен буде відправити посилений запит одному зі своїх сусідів, який знову може бути обраний як перший, який отримав дані щодо відповідного запиту. Таким чином, емпірично низький шлях з низькою затримкою поступово посилюється і стає домінуючим шляхом передачі даних від джерела до приймача. Оскільки всі запити мають термін дії, негативне підкріплення може бути застосоване шляхом простої відмови від повторного запиту по непродуктивних шляхах. Точні способи

застосування позитивного та негативного підкріплення можуть бути досить складними. Протокол повинен забезпечувати баланс між ефективністю в стабільних умовах (використовуючи лише найкращий доступний шлях) і реакцією на умови, що змінюються, що вимагає постійної доступності даних про якість кількох шляхів [4].

Хоча у даному випадку було тільки одне джерело і один приймач, спрямована дифузія однаково добре працює для передачі між кількома джерелами і приймачами, як в одноадресному, так і в багатоадресному режимі. Слід також відзначити, що, хоча наш сценарій зіставлення джерела і приймача був типу «запит даних» (всі комунікації відбувалися на запит приймача), спрямована дифузія досить універсальна, щоб допускати і «проштовхування» даних, дозволяючи сенсорним вузлам запускати поширення подій, коли вони виявляють щось, що, на їх думку може представляти інтерес для приймачів. Агрегація даних, що надходять з кількох джерел одного приймача, також легко підтримується в рамках спрямованої дифузії.

1.3 Протокол RR

Rumor Routing (RR) – це ще одна покращена версія алгоритму спрямованої дифузії. Головна мета алгоритму – заповнити область між потоком запитів та потоком подій. Він корисний, якщо кількість запитів, порівняно з кількістю подій, знаходиться між двома точками перетину. Іншими словами, він поширює події, якщо їх кількість мала, а кількість запитів велика, а отже, обробляє потік подій і потік запитів. Він робить це для того, щоб надсилати запити до вузлів, які виявили конкретну подію, а не поширювати їх по всій мережі для доступу до конкретної інформації про подію, що відбувається. В алгоритмі кожен вузол підтримує список своїх сусідів, а також таблицю подій з інформацією про пересилання всім відомим подіям. Список сусідів може створюватися та підтримуватись активно шляхом активної трансляції запиту або пасивно, шляхом прослуховування трансляцій інших вузлів. Алгоритм протестували на статичній

топології, де кожен вузол просто передавав свій ідентифікатор на початку процесу маршрутизації.

Коли вузол фіксує подію, він додає в свою таблицю подій з нульовою відстанню до події. Він також ймовірно генерує агента. Агент є довгоживучим пакетом, який переміщається по мережі, поширюючи інформацію про локальні події на віддалені вузли. Він містить таблицю подій, аналогічну до таблиці вузлів, яку він синхронізує з кожним відвіданим вузлом. Агент переміщається через мережу на певну кількість переходів (La), а потім вмирає. Будь-який вузол може згенерувати запит, який має бути спрямований до певної події. Якщо вузл має маршрут до події, він передасть запит. Якщо ні, він надішле запит у випадковому напрямку. Це продовжується до закінчення часу життя запиту (Lq) або доти, доки запит не досягне вузла, який зафіксував цільову подію. Якщо вузол, який ініціював запит, визначає, що запит не досяг пункту призначення, він намагається повторно передати його, відмовляється від нього або розсилає його далі. Протокол гарантує, що між джерелом та приймачем використовується лише один шлях, на відміну від DD, де дані можуть передаватися кількома шляхами з низькою швидкістю. Він працює краще, коли обсяг даних невеликий [4,5].

1.4 Протокол LEACH

Для подолання недоліків традиційних протоколів маршрутизації та розповсюдження даних, які працюють поверх не багаторівневих чи плоских мережних архітектур, було запропоновано протокол з урахуванням кластеризації, Так званий з адаптивною ієрархією кластеризації з низьким енергоспоживанням Low Energy Adaptive Clustering Hierarchy (LEACH). LEACH заснований на методі агрегації (або злиття), який поєднує або агрегує вихідні дані дані меншого розміру, що несуть лише значну інформацію про всіх окремі датчики. З цією метою LEACH ділить мережу на кілька кластерів датчиків, які створюються з використанням локалізованої координації та управління не тільки для зменшення обсягу даних, що передаються на приймач, але й для підвищення

масштабованості та надійності маршрутизації та поширення даних. Враховуючи, що розсіювання енергії датчиками залежить від відстані та розміру переданих даних, LEACH прагне передавати дані на короткі відстані та зменшити кількість операцій передачі та прийому. У LEACH головні вузли кластерів не вибираються статичним чином, в протилежному випадку вони швидко розрядять свою енергію і вийдуть із ладу. Натомість LEACH використовує випадкове обертання положення головного вузла кластера з високою енергією, щоб дати можливість усім датчикам діяти як головні вузли кластера і уникнути розрядки батареї окремого датчика. Робота LEACH поділена на раунди, кожен з яких має в основному дві фази: фазу налаштування організації мережі в кластери і фазу стійкого стану передачі даних на приймач. Головні вузли кластерів використовують протокол CSMA MAC для оголошення свого стану. Таким чином, всі датчики, які не є головними вузлами кластера, повинні тримати свої приймачі увімкненими під час фази налаштування, щоб чути оголошення, що надсилаються головними вузлами кластеру. Ці кластерні лідери вибираються ними самими з деякою ймовірністю та передають інформацію про свій статус іншим датчикам у мережі. Рішення про те, чи стане датчик кластерним лідером, приймається незалежно без будь-яких переговорів з іншими датчиками. Зокрема, датчик приймає рішення стати кластерним лідером на основі бажаного відсотка кластерних лідерів (певного заздалегідь), поточного раунду та набору датчиків, які не стали кластерними лідерами протягом останніх раундів.

Серед усіх оголошених головних вузлів кластера датчик вибирає найближчий, який забезпечить мінімальне енергоспоживання при передачі даних, а потім повідомляє свого головного вузла кластера про свій рішення приєднатися до кластера, використовуючи протокол CSMA MAC. Аналогічно, головні вузли кластера повинні тримати свої приймачі увімкненими, щоб чути ці повідомлення про приєднання. Після того, як мережу розділено на кластери, головний вузол кластера обчислює розклад TDMA для своїх датчиків, вказівник, коли датчику в кластері дозволено відправляти свої дані. Таким чином, датчик буде включати свій радіомодуль тільки тоді, коли йому буде дозволено передавати дані

відповідно до розкладу, встановленого його головним вузлом кластера, що спричинить значну економію енергії. Крім того, LEACH забезпечує злиття даних у кожному кластері шляхом агрегування даних, щоб зменшити загальний обсяг даних перед відправкою в приймач. Іншими словами, після того, як головний вузол кластера збере всі дані зі своїх датчиків, він агрегує їх і передає агреговані дані приймачеві [6,7].

LEACH можна розглядати як гібридний підхід, який використовує пересилання даних на короткі та довгі відстані. Датчики всередині кластера передають отримані дані на короткі відстані, тоді як головні вузли кластера взаємодіють безпосередньо з приймачем. Хоча LEACH допомагає датчикам усередині кластера повільно розсіювати енергію, головні вузли кластера споживають більше енергії, коли вони розташовані далі від приймача. Пряме надсилання даних приймачеві є основною проблемою LEACH. Найкращий підхід, це дозволити багатокрокову передачу даних приймачеві через інші головні вузли кластера. У цьому випадку головному вузлу кластера не потрібно оновлювати агреговані дані від інших головних вузлів кластера, а лише надсилати їх приймачеві. Більш того, при ухваленні рішення про те, чи стане датчик головним вузлом кластера, слід враховувати залишкову енергію цього датчика.

1.5 Протокол TEEN

Для критично важливих за часом програм реактивна мережа більш підходить, ніж проактивна мережа. Для динамічного компромісу між енергоефективністю, точністю даних та часом відгуку було запропоновано протокол зв'язку, званий пороговим енергетично ефективним протоколом сенсорної мережі Threshold Sensitive Energy Efficient Sensor Network Protocol (TEEN). TEEN використовує ієрархічну кластеризацію, яка групує датчики кластери, кожен із яких очолює головний кластер. Датчики всередині кластера передають свої дані чолі кластера. Головний кластер надсилає агреговані дані головним кластерам вищого рівня до тих пір, поки дані не досягнуть приймача.

Таким чином, TEEN - це протокол зв'язку для кластеризації, орієнтований на реактивну мережу і що дозволяє головам кластерів накладати обмеження те що, коли датчики повинні передавати свої дані. Кожен головний кластер передає своїм членам значення, зване жорстким порогом (HT), для вимірюваного атрибута, після перевищення якого датчик повинен увімкнути свій передавач, щоб передати свої дані на чолі кластера. Крім того, головний вузол кластера передає ще одне значення, зване м'яким порогом (ST), яке вказує на невелику зміну значення вимірюваного атрибуту, що запускає включення передавача датчика та відправлення виміряних даних головному вузлу кластера. Датчики всередині кластера можуть бути заплановані за допомогою TDMA або CDMA, щоб уникнути колізій у кластері. Однак це призведе до затримки при передачі критично важливих за часом даних приймачеві [6,8].

Слід зазначити, що TEEN не підходить для програм датчиків, що вимагають від датчиків регулярної передачі даних.

1.6 Протокол PEGASIS

Для покращення LEACH був запропонований інший протокол, званий енергоефективним збором інформації в сенсорних інформаційних системах Power-Efficient Gathering in Sensor Information Systems (PEGASIS), який дозволяє лише одному кластерному головному пристрою передавати дані приймачеві в кожному раунді. Більше того, датчик повинен передавати дані своїм локальним сусідам на етапі злиття даних, а не надсилати їх безпосередньо своєму кластерному головному пристрою, як у випадку LEACH. У PEGASIS датчики організовані таким чином, щоб сформувати ланцюжок, який може бути сформований самими датчиками з використанням алгоритму пошуку, або приймачем, який повинен транслювати ланцюжок всім датчикам в мережі. На етапі побудови передбачається, що всі датчики мають глобальні знання про мережу, зокрема, про місцезнаходження датчиків, і використовується пошуковий підхід. Зокрема, процес починається з найдальшого від приймача датчика, щоб

гарантувати, що датчики, розташовані далі від приймача, мають близьких сусідів. Коли датчик виходить з ладу або ламається через низький заряд батареї, ланцюжок будується з використанням того ж пошукового підходу, минаючи вийшовший з ладу датчик. Ланцюжок має два кінцеві датчики, і на кожному етапі злиття даних лише один головний (тобто датчик, відповідальний за передачу об'єднаних даних до приймача) буде передавати об'єднані дані до приймача. Будь-який інший проміжний датчик об'єднає дані, отримані від свого сусіда, зі своїми власними даними та передасть об'єднані дані своєму сусідові, розташованому ближче до приймача, ніж він сам, щоб об'єднані дані були перенаправлені у бік приймача. Зверніть увагу, що всі датчики братимуть участь у злитті даних, крім кінцевих датчиків, якщо вони не є лідерами, які будуть передавати об'єднані дані в приймач. Етап злиття даних у кожному раунді вимагає, щоб лідер відправив керуючий токен кінцевим датчикам ланцюжка, де має початися передача даних. В кінці головний отримує два об'єднані набори даних з обох сторін ланцюжка, об'єднує їх зі своїми власними даними та передає остаточні об'єднані дані приймачеві [6,9].

1.7Протокол SOP

SOP (Self-Organization Protocol) є протоколом маршрутизації, що ґрунтується на принципах самоорганізації в сенсорних мережах і спрямований на забезпечення ефективної та надійної роботи системи в умовах нерівномірного або неоднорідного розташування вузлів. Його архітектура передбачає організацію взаємодії між мобільними чи стаціонарними сенсорними вузлами та стаціонарними вузлами-роутерами, які виконують роль опорних елементів маршрутизації.

Функціонування SOP базується на тому, що сенсорний вузол може стати частиною мережі лише за умови можливості передавання власних даних щонайменше до одного роутера – безпосередньо або через проміжні вузли. У результаті мережа формується навколо роутерів, що забезпечують централізовану

організацію та стабільні маршрути передавання даних. Протокол підтримує роботу в гетерогенних мережах, у яких вузли відрізняються за обчислювальними можливостями, енергетичними ресурсами та функціональними ролями.

Важливою особливістю SOP є обов'язкова адресація кожного вузла, що гарантує унікальну ідентифікацію пристроїв і коректність передавання даних. Це робить протокол доцільним для застосувань, де необхідний обмін інформацією з конкретними вузлами або отримання даних від визначених пристроїв. Архітектура SOP забезпечує балансування навантаження між роутерами та сенсорними вузлами, сприяючи енергоефективному передаванню даних і зменшенню витрат на маршрутизацію завдяки обмеженому розміру таблиць маршрутів. У разі порушення зв'язку або зміни топології мережі протокол виконує локальну перебудову маршрутів без потреби глобального оновлення всієї мережі.

SOP є придатним для використання в системах, де критично важливо підтримувати зв'язок із визначеними вузлами або об'єктами, зокрема в задачах точкового моніторингу, промислових сенсорних мережах, логістичних системах, а також під час побудови сенсорних мереж зі змішаними типами вузлів – мобільними та стаціонарними [10].

1.8 Протокол GAF

Geographic Adaptive Fidelity (GAF) – це протокол маршрутизації, запропонований для мобільних однорангових мереж (MANET). Хоча він був запропонований для MANET, він сприяє енергозбереженню і, отже, може використовуватися для сенсорних бездротових мереж (WSN). Розробка GAF мотивована результатами попередніх досліджень, заснованих на енергетичній моделі, яка враховує споживання енергії через прийом та передачу пакетів, а також час простою (або прослуховування), коли радіомодуль сенсора (вузла) включений для виявлення вхідних пакетів. Ці дослідження [11,12] показали, що вузли з батарейним живленням споживають енергію не тільки під час прийому

або відправлення пакетів, але й під час прослуховування чи простою. Тому недостатньо оптимізувати споживання енергії лише за рахунок скорочення передачі та прийому пакетів. Крім того, радіомодуль також має бути вимкнений. GAF базується на цьому механізмі; тобто на відключенні непотрібних сенсорів при збереженні постійного рівня точності маршрутизації (або безперервного зв'язку між сенсорами, що взаємодіють).

GAF ділить поле датчиків на квадрати сітки, і кожен датчик використовує інформацію про своє місцезнаходження, яка може бути надана GPS або іншими системами позиціонування для прив'язки до певної сітки, де він перебуває. Цей тип прив'язки використовується GAF для ідентифікації датчиків, які є еквівалентними з точки зору пересилання пакетів. Розмір квадрата сітки вибирається таким чином, щоб датчики в одній сітці були еквівалентними з точки зору маршрутизації, і щоб датчики у сусідніх сітках могли взаємодіяти один з одним. Таким чином, еквівалентні датчики можуть координувати свої дії для визначення енергоефективного графіка своєї діяльності, який визначає, коли і як довго датчики залишаються пильними або сплячими [6].

Як показано на рис. 1.4, діаграма переходів станів GAF має три стани: виявлення, активність та сон. Коли датчик переходить у сплячий стан, він відключає свій радіомодуль для економії енергії. У стані виявлення датчик обмінюється повідомленнями про виявлення, щоб дізнатися про інші датчики тієї ж мережі. Навіть в активному стані датчик періодично передає повідомлення про виявлення, щоб інформувати еквівалентні датчики про свій стан. Час, проведений у кожному з цих станів, може бути налаштований програмою залежно від кількох факторів, таких як його потреби та мобільність датчика. GAF прагне максимізувати термін служби мережі, досягаючи стану, в якому в кожній мережі є лише один активний датчик на основі правил ранжування датчиків. Ранжування датчиків ґрунтується на рівнях їх залишкової енергії. Таким чином, датчик із вищим рангом зможе обробляти маршрутизацію в межах відповідних мереж.

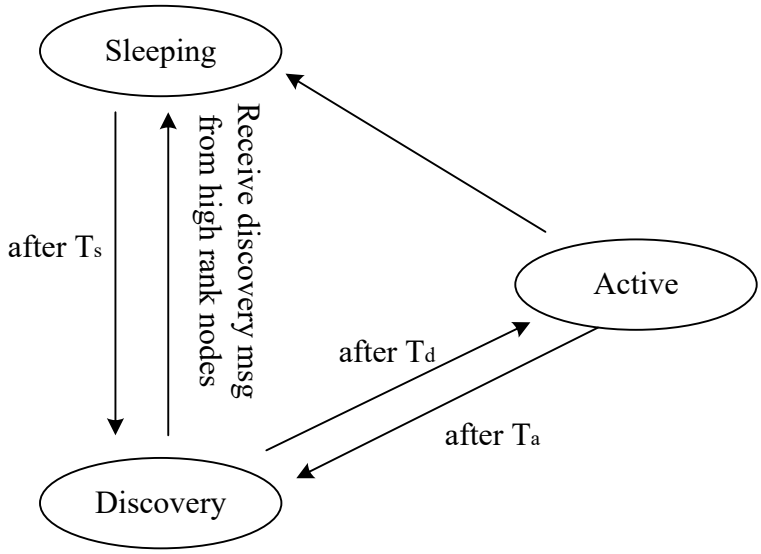

Рисунок 1.4 – Діаграма переходу станів GAF

Наприклад, датчик в активному стані має вищий ранг, ніж датчик у стані виявлення. Датчик з тривалішим очікуваним терміном служби має більш високий ранг. Щоб усі датчики працювали якомога довше без шкоди для будь-якого з них, GAF використовує стратегію балансування навантаження, коли датчик залишається в активному стані лише деякий час, перш ніж переключитися в сплячий режим. Це дає можливість іншим датчикам у тій самій мережі активуватись та обробляти маршрути. Обгрунтування цього правила полягає в тому, що датчики, що переходять у стан виявлення, матимуть менше залишкової енергії, ніж їхні сусіди в режимі сну, де вони економлять енергію. Слід зазначити, що переміщення датчиків може призвести до того, що мережі взагалі не залишиться активних датчиків. Для вирішення цієї проблеми датчик оцінює час, коли він планує залишити свою мережу, на основі даних свого приймача GPS, і передає цей час у своєму повідомленні про виявлення. Після отримання цього повідомлення сусіди датчика коригують час свого сплячого режиму таким чином, щоб у мережі завжди був один активний датчик для обробки маршрутів всередині цієї мережі [6].

1.9 Протокол GEAR

Запропоновано енергоефективний протокол маршрутизації, який називається географічною та енергоефективною маршрутизацією Geographicand Energy – Aware Routing (GEAR), для маршрутизації запитів до цільових регіонів у сенсорному полі. У GEAR передбачається, що датчики оснащені обладнанням локалізації, наприклад GPS-модулем або системою локалізації, щоб знати своє поточне місцезнаходження. Крім того, датчики знають свою залишкову енергію, а також місце розташування та залишкову енергію кожного зі своїх сусідів. GEAR використовує енергоефективну евристику, засновану на географічній інформації, для вибору датчиків, які маршрутизуватимуть пакет у цільовий регіон. Потім GEAR використовує рекурсивний географічний алгоритм пересилання поширення пакета всередині цільового регіону. Мета використання енергоефективного поширення даних із географічною інформацією полягає в тому, щоб допомогти приймати енергоефективні рішення щодо маршрутизації. Розробка GEAR обумовлена тим фактом, що в ряді систем, що враховують розташування, таких як бездротові сенсорні мережі (WSN), корисно поширювати інформацію в межах географічного регіону. Наприклад, користувач може запитати у сенсорної програми інформацію про температуру в заданому регіоні протягом певного часового інтервалу. Щоб отримати відповідь, цей запит має бути надіслано на датчики, розташовані у цільовому регіоні. Інформація про місцезнаходження, додана до запиту, допоможе відправити його безпосередньо до кінцевої зони призначення, а не поширювати його по всьому полю датчиків. Для кожного зі своїх сусідів датчик підтримує дві змінні, які називають оціночною вартістю та вивченою вартістю. Оцінна вартість сусіда залежить від споживаної енергії і відстані між нею і центром цільового регіону. Якщо датчик не має вивченої вартості для свого сусіда, він обчислює оцінну вартість як значення за промовчанням для вивченої вартості. Датчик вибирає сусіда з мінімальною вивченою вартістю, щоб збалансувати енергоспоживання всіх своїх сусідів. Після

процесу вибору датчик встановлює свою власну вивчену вартість дорівнює сумі вивченої вартості та вартості передачі пакету [6].

GEAR складається з двох основних фаз: пересилання пакета в регіон призначення (фаза 1) та розповсюдження пакета всередині регіону призначення (фаза 2). У фазі 1 датчик вибирає сусіда, який знаходиться ближче до регіону призначення, ніж він сам, щоб той виступав як наступний пристрій, що пересилає. В іншому випадку всі його сусіди знаходяться далі від регіону призначення, ніж він сам, і, отже, між датчиком, що містить пакет, та цільовим регіоном утворюється порожня область (рис. 1.5).

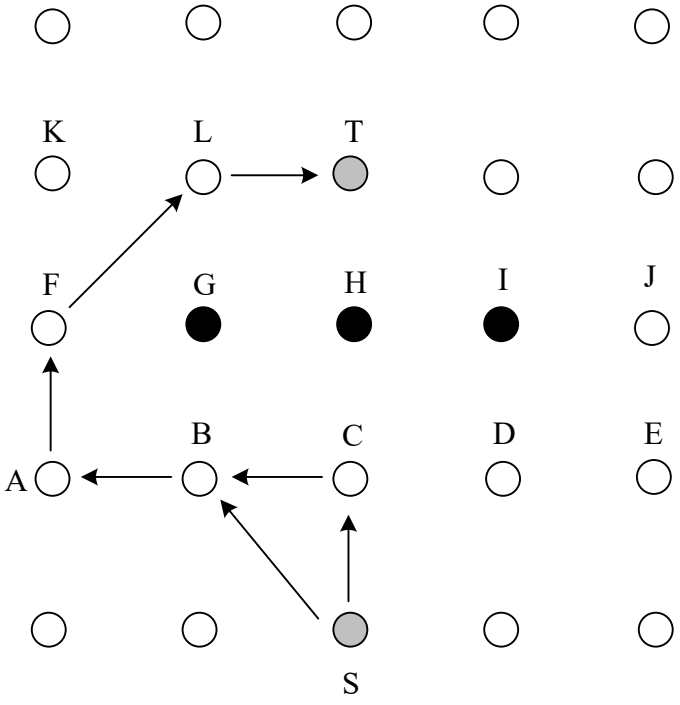

Рисунок 1.5 – Маршрутизація з обходом перешкод

У цьому випадку GEAR вибирає одного з тих сусідів, чия вивчена вартість є мінімальною. На другому етапі GEAR використовує рекурсивний географічний алгоритм пересилання для розповсюдження пакета у межах цільового регіону. У цьому випадку цільовий регіон поділяється на чотири підрегіони, і поточний датчик створює чотири копії пакета для одноадресної розсилки до цих

підрегіонів. Ця процедура поділу і пересилання повторюється до тих пір, поки поточний вузол не виявиться єдиним усередині цього підрегіону, і, отже, пакет відкидається. Коли датчики розгорнуті рідко, GEAR використовує обмежену розсилку, яка енергоефективніша, ніж рекурсивне географічне пересилання. У цьому випадку датчик відправляє лише одне широкомовне повідомлення всім своїм сусідам [6].

Слід зазначити, що GEAR можна також класифікувати як протокол поширення даних, орієнтований на дані.

1.10 Протокол SAR

Маршрутизація з послідовним призначенням Sequential Assignment Routing (SAR), є одним із перших протоколів маршрутизації для бездротових сенсорних мереж, в якому рішення про маршрутизацію вводиться поняття QoS. Рішення про маршрутизацію до SAR залежить від трьох факторів: енергетичних ресурсів, QoS на кожному шляху та рівня пріоритету кожного пакета. Щоб уникнути збою одного маршруту, використовується багатоколійний підхід та локалізовані схеми відновлення шляху. Для створення кількох шляхів від вихідного вузла будується дерево з коренем у вихідному вузлі до вузлів призначення (тобто безлічі) базових станцій (БС). Шляхи дерева будуються за винятком вузлів з низьким енергоспоживанням або гарантією QoS. Наприкінці цього процесу кожен сенсорний вузол буде частиною багатоколійного дерева. Таким чином, SAR – це багатоколійний протокол, керований таблицями, метою якого є досягнення енергоефективності та відмовостійкості. По суті, SAR обчислює зважену метрику QoS як добуток адитивної метрики QoS та вагового коефіцієнта, пов'язаного з рівнем пріоритету пакета. Мета алгоритму SAR – мінімізувати середню зважену метрику QoS протягом усього терміну служби мережі. Якщо топологія змінюється через збої вузлів, потрібно перерахунок шляху. Як превентивний захід базова станція періодично запускає перерахунок шляхів, щоб врахувати будь-які зміни в топології. Для відновлення після збою використовується процедура

підтвердження зв'язку, що базується на схемі локального відновлення шляху між сусідніми вузлами. Відновлення після збою здійснюється шляхом забезпечення узгодженості таблиць маршрутизації між висхідними та низхідними вузлами на кожному шляху. Результати моделювання показали, що SAR забезпечує менше енергоспоживання, ніж алгоритм мінімальної енергетичної метрики, який фокусується лише на енергоспоживання кожного пакета без врахування його пріоритету. SAR підтримує декілька шляхів від вузлів до базової станції. Хоча це забезпечує відмовостійкість та простоту відновлення, протокол страждає від накладних витрат на підтримку таблиць та станів на кожному вузлі датчика, особливо коли кількість вузлів велика [6].

1.11 Протокол SPEED

Stateless Protocol for End-to-end Estimation of Delay (SPEED) – протокол маршрутизації QoS для сенсорних мереж, який забезпечує наскрізну гарантію (end-to-end) у реальному часі. Протокол вимагає від кожного вузла підтримувати інформацію про своїх сусідів і використовує географічне пересилання для пошуку шляхів. А також підтримує кращу швидкість доставки в сенсорних мережах шляхом локального регулювання пакетів, що відправляються на рівень MAC, та перенаправлення трафіку на мережному рівні [13-15].

1.12 Аналіз протоколів маршрутизації сенсорних мереж

Sensor Protocols for Information via Negotiation (SPIN). Протоколи SPIN базуються на двох основних механізмах – узгодженні та адаптації використання ресурсів. Перед передаванням даних у мережі SPIN дає змогу сенсорам попередньо домовлятися між собою, що дозволяє уникнути поширення зайвої або дубльованої інформації. Для опису даних, які передаються сенсорами, у SPIN застосовуються метадані. Використання метаданих допомагає запобігти виникненню надлишкового дублювання інформації для окремого сенсора.

Direcied Diffusion – протокол включає кілька ключових складових, зокрема механізми іменування даних, інтереси та градієнти, поширення інформації й етап зміцнення. Передавання даних у межах такого підходу реалізується за принципом спрямованої дифузії. На початковому етапі приймач задає невисоку швидкість передавання даних для всіх виявлених подій. Надалі він може «зміцнити» конкретний сенсор, надавши йому дозвіл збільшити швидкість передавання шляхом надсилання відповідного повідомлення-інтересу. Якщо сусідній сенсор отримує таке повідомлення та визначає, що запропонована швидкість передавання є вищою за попередню і перевищує швидкість будь-якого наявного градієнта, він, у свою чергу, виконує зміцнення одного або кількох своїх сусідніх сенсорів [16].

У результаті спрямована дифузія надає універсальний механізм зв'язку для сенсорних мереж. На відміну від традиційних мереж, які прагнуть забезпечити прямі канали зв'язку, спрямована дифузія орієнтована на дані у своєму мережевому поданні та приймає всі рішення щодо маршрутизації за допомогою локальних взаємодій між сусідами. Вона забезпечує реактивний метод маршрутизації, виявляючи маршрути між джерелами та приймачами інформації в міру необхідності. Однак завдяки орієнтованому на дані підходу дані або запити даних поширюються в рамках процесу виявлення маршруту. Після виявлення відповідних шляхів можна використовувати градієнтний механізм для концентрації трафіку вздовж оптимальних шляхів, при цьому завжди зберігаючи достатній периферійний огляд змін у мережі, щоб забезпечити швидку адаптацію нових топологій або нових вимог. Спрямована дифузія, це також високоефективний з погляду енергоспоживання протокол, навіть у порівнянні з протоколами, що використовують попередньо обчислені маршрути для зв'язку джерел та приймачів (всезнаючі дерева багатоадресної розсилки найкоротших шляхів). Це пов'язано з тим, що спрямована дифузія може ефективно пригнічувати події, що дублюють, і виконувати агрегацію інформації всередині мережі [6].

Rumor Routing. Основним механізмом протоколу є агент-пакет із тривалим часом життя, який переміщується мережею та інформує кожен сенсор про події, зафіксовані ним під час проходження мережі. Агент поширюється лише до заданої кількості переходів (hop'ів), після чого його робота завершується. Кожен сенсор, так само як і сам агент, зберігає перелік подій у вигляді пар «подія–відстань», де відстань визначається кількістю hop'ів до відповідної події від сенсора, який її зафіксував. Під час взаємодії агента з сенсорами відбувається синхронізація цих списків, у результаті чого кожен сенсор отримує інформацію про найкоротші шляхи до подій, що виникають у мережі.

Low Energy Adaptive Clustering Hierarchy (LEACH). В алгоритмі LEACH роль голови кластера періодично переходить між різними вузлами мережі, що забезпечує більш рівномірне споживання енергетичних ресурсів. Однією з основних переваг LEACH є використання циклічної організації роботи. У межах кожного циклу новий голова кластера обирається серед вузлів, які раніше не виконували цю роль, що дає змогу підтримувати необхідну частку кластерних голів відносно загальної кількості вузлів у мережі. Після обрання голова кластера формує та поширює розклад доступу з часовим поділом (TDMA) для вузлів свого кластера. Завдяки цьому вузли здійснюють передавання даних лише у відведений для них час. Крім того, голова кластера виконує агрегацію отриманих даних з метою зменшення надмірності інформації [16].

Threshold Sensitive Energy Efficient Sensor Network Protocol (TEEN) на відміну від ієрархічних протоколів, цей підхід орієнтований на реактивні мережі, які повинні оперативно реагувати на зміни різних параметрів. У межах протоколу голова кластера розповсюджує порогові значення двох типів – жорстке (hard) та м'яке (soft). Передавання даних відбувається лише у разі досягнення цих порогів. Якщо певний параметр із набору атрибутів перевищує жорстке порогове значення, вузол активує передавач і надсилає інформацію. Подальше передавання даних іншими вузлами здійснюється у визначені часові інтервали за умови, що поточне значення параметра перевищує hard-поріг, а його зміна відносно

попереднього значення є не меншою за soft-поріг. Обидва механізми спрямовані на зниження енергоспоживання, пов’язаного з передаванням повідомлень.
Основним недоліком цього алгоритму є те, що у випадку недосягнення контрольованими параметрами порогових значень обмін даними між вузлами не відбувається. У такій ситуації користувач не отримує жодної інформації та не може оцінити працездатність мережі. Тому цей алгоритм доцільно застосовувати в додатках, де передавання даних має бути регулярно.

Power-Efficient Gathering in Sensor Information Systems (PEGASIS) інша краща версія алгоритму LEACH. Замість об’єднання вузлів у кластери в цьому підході використовується формування ланцюжків сенсорних вузлів. У межах такої структури кожен вузол обмінюється даними лише з одним найближчим сусідом, що дає змогу оптимально налаштовувати потужність передавання. Кожен вузол виконує агрегацію отриманих даних і послідовно передає їх уздовж ланцюжка у напрямку базової станції. Протягом одного циклу лише один вузол із ланцюжка безпосередньо взаємодіє з базовою станцією. Сам ланцюжок формується з урахуванням мінімізації енергетичних витрат.

Self-Organizing Protocol (SOP). Протокол маршрутизації та самоорганізації призначений для використання в гетерогенних сенсорних мережах і підтримує як стаціонарні, так і мобільні вузли. Кінцеві сенсори, що збирають дані про параметри навколишнього середовища, передають отриману інформацію визначеній кількості вузлів, які виконують функції маршрутизаторів. Ці вузли є стаціонарними та формують базову комунікаційну інфраструктуру мережі. Надалі зібрані дані пересилаються маршрутизаторами на більш потужні базові станції. Кожен крайовий вузол повинен мати можливість встановити зв’язок щонайменше з одним шлюзом, щоб бути повноцінною частиною сенсорної мережі. Ідентифікація кінцевих вузлів може здійснюватися за адресою маршрутизатора, через який вони передають дані. У результаті формується ієрархічна архітектура, у межах якої групи вузлів можуть динамічно створюватися та об’єднуватися залежно від потреб [16].

Geographic Adaptive Fidelity (GAF). Цей протокол належить до енергозберігаючих і ґрунтується на принципі проєктування віртуальної ґратки розташування сенсорних вузлів, координати яких визначаються за допомогою GPS або інших систем позиціонування. Таке подання дає змогу оцінювати вартість маршрутизації пакета до цільового вузла, де вартість визначається обсягом енергетичних витрат на його передавання відповідно до прийнятої енергетичної моделі. Чим далі знаходиться квадрант, у якому розташований вузол-призначення, тим вищими є витрати на маршрутизацію. Водночас усі вузли, що знаходяться в межах одного квадранта, мають однакову вартість передавання пакета до них.

Geographicand Energy – Aware Routing (GEAR). Алгоритм маршрутизації базується на тому, що кожен вузол володіє інформацією про власне місцеположення, отриманою за допомогою GPS або інших систем позиціонування, і здійснює евристичний вибір маршруту передавання серед множини сусідніх вузлів. Для доставки пакетів у межах сенсорного поля GEAR застосовує рекурсивний алгоритм географічної естафетної передачі, який послідовно пересилає дані від вузла до вузла з урахуванням їх просторового розташування.

Sequential Assignment Routing (SAR). Це один із перших протоколів маршрутизації для бездротових сенсорних мереж, що забезпечує підтримку критеріїв Quality of Service (QoS – якості обслуговування). Він ґрунтується на призначенні атрибутів рівня пріоритету для кожного пакета. Крім того, зв’язки та маршрути оцінюються за метрикою, що характеризує їх здатність забезпечувати необхідний рівень обслуговування, враховуючи затримки та енергетичні витрати. На основі цього алгоритму формується дерево маршрутів із коренем на відстані одного hop від базової станції, при цьому враховуються пріоритети пакетів, енергетичні ресурси вузлів та показники QoS. Протокол також періодично оновлює маршрути для забезпечення стабільності мережі у разі виходу з ладу будь-якого активного вузла [16].

Ще одним протоколом, орієнтованим на якість обслуговування, є SPEED. Для його роботи кожен вузол зберігає інформацію про своїх сусідів і використовує дані про їхнє географічне розташування для пошуку маршрутів. Протокол намагається забезпечити певну швидкість доставки пакетів, що дозволяє заздалегідь оцінювати час проходження даних від відправника до отримувача, розділивши відстань на швидкість пакета. SPEED також підтримує обхідні маршрути у випадку перевантажень мережі. Модуль маршрутизації протоколу, названий Stateless Geographic Non-Deterministic Forwarding (SNFG), працює разом із чотирма іншими модулями мережного рівня. Оцінка затримки на кожному вузлі базується на вимірюванні часу, що минув після запиту підтвердження отримання пакета. Виходячи з цієї затримки, SNFG обирає вузол, який відповідає вимогам по швидкості обробки. У випадку, якщо такого немає, розглядаються сусідні вузли [1, 16].

У табл. 1.1 наведено характеристики для одинадцяти протоколів маршрутизації.

Таблиця 1.1 – Узагальнені характеристики розглянутих протоколів маршрутизації

№	Протоколи маршрутизації	Мобільність	Споживна потужність	Узгодженість	Агрегація даних	Локалізація	QoS	Складність структури	Масштабованість	Множинність шляхів
N1	SPIN	можлива	обмежена	присутня	присутня	відсутня	відсутня	низька	обмежена	присутня
N2	DD	обмежена	обмежена	присутня	присутня	відсутня	відсутня	низька	обмежена	присутня
N3	RR	дуже обмежена	не визначена	відсутня	присутня	відсутня	відсутня	низька	хороша	відсутня
N4	LEACH	фіксовані БС	максимальна	відсутня	присутня	присутня	відсутня	головні вузли кластера	хороша	відсутня
N5	TEEN	фіксовані БС	мінімальна	відсутня	присутня	відсутня	відсутня	головні вузли кластера	хороша	відсутня

Продовження таблиці 1.1

N6	PEGASIS	фіксовані БС	максимальна	відсутня	відсутня	присутня	відсутня	низька	хороша	відсутня
N7	SOP	відсутня	не визначена	відсутня	відсутня	відсутня	відсутня	низька	низька	відсутня
N8	GAF	обмежена	обмежена	відсутня	відсутня	присутня	відсутня	низька	хороша	відсутня
N9	GEAR	обмежена	обмежена	відсутня	відсутня	присутня	відсутня	низька	обмежена	відсутня
N10	SAR	відсутня	не визначена	присутня	присутня	відсутня	присутня	середня	обмежена	відсутня
N11	SPEED	відсутня	не визначена	відсутня	відсутня	присутня	присутня	середня	обмежена	присутня

2 ОГЛЯД МЕТОДІВ АНАЛІЗУ ПРОТОКОЛІВ

2.1 Метод аналізу ієрархій

Метод аналізу ієрархій Т. Сааті (MAI) ґрунтується на декомпозиції задачі вибору найкращого варіанта системи на окремі елементи з подальшим визначенням їх відносної важливості. Оцінювання здійснюється за допомогою експертних попарних порівнянь компонентів системи, результати яких обробляються із застосуванням відповідного математичного апарату для формування вектора пріоритетів. Отримані значення дають змогу встановити альтернативу проєктованої системи, що має найбільшу перевагу серед розглянутих варіантів.

Побудова ієрархічної моделі системи дозволяє відстежити вплив змін пріоритетів на верхніх рівнях на показники нижчих рівнів. Такий підхід сприяє більш ґрунтовному розумінню структури та функціональних характеристик системи, а також забезпечує можливість аналізу чинників впливу й відповідних цілей на кожному рівні ієрархії.

На рис. 2.1 наведено детальну ієрархічну структуру задачі вибору, яка формується від верхнього рівня, що відображає загальну мету, через проміжні рівні, котрі характеризують показники якості системи, до найнижчого рівня. У MAI ключовим є принцип попарного порівняння, відповідно до якого експерти визначають відносну важливість об’єктів вибору шляхом їх порівняння між собою у парах. Оцінюванню підлягають як альтернативні варіанти системи (на третьому рівні), так і показники їхньої якості (на другому рівні). Результати експертних оцінок подаються у вигляді матриці (2.1), що відображаються числовими показниками згідно зі шкалою відносної важливості, поданою в табл. 2.1. [17].

$$A = \begin{pmatrix} a_{11}a_{12}...a_{1j} \\ a_{21}a_{22}...a_{2j} \\ ... \\ a_{i1}a_{i2}...a_{ij} \end{pmatrix}, \qquad (2.1)$$

де a_{ij} – оцінки порівнянь елементів.

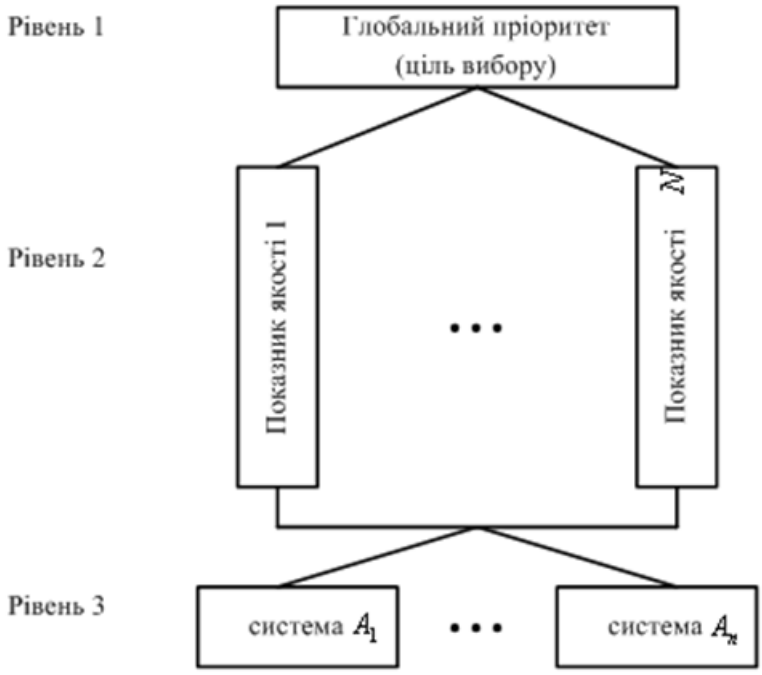

Рисунок 2.1 – Ієрархічне структура задачі вибору

Наступним етапом дослідження є детальний аналіз матриць попарних порівнянь елементів ієрархії другого та третього рівнів, у межах якого здійснюється обчислення вектора пріоритетів [18]. Компоненти цього вектора визначаються як геометричне середнє значень елементів рядків матриці попарних порівнянь відповідного рівня ієрархії (2.2)

$$V_i = \sqrt[n]{\Pi_{k=1}^{n} \frac{w_i}{w_k}}, \qquad P_i = \frac{V_i}{S}, \qquad (2.2)$$

де $S = \sum_{i=1}^{n} V_i$, P_i – пріоритети елементів.

Таблиця 2.1 – Шкала оцінювання рівня важливості елементів

Інтенсивність відносної важливості	Визначення
1	Рівна важливість
3	Помірне перевагу одного над іншим
5	Значна або сильна перевага
7	Значна перевага
9	Дуже сильна перевага
2,4,6,8	Проміжні рішення між двома судженнями
Зворотні величини наведених вище чисел	Якщо при порівнянні одного виду елемента з іншим отримано одне з вищевказаних чисел, то при порівнянні другого елементу з першим отримаємо зворотну величину

2.2 Метод експертного оцінювання

Методи експертного оцінювання ґрунтуються на узагальненні кількісних та/або якісних суджень фахівців з метою обґрунтування управлінських і проєктних рішень. Експертиза передбачає групове оцінювання об’єктів та їхніх характеристик, після чого здійснюється обробка й аналіз отриманих результатів. Основна увага приділяється перевірці узгодженості експертних оцінок та виявленню можливих розбіжностей у думках експертів.

Якщо результати експертизи не дозволяють ухвалити рішення, процедуру повторюють із роз’ясненням розбіжностей до досягнення задовільного узгодження, як, наприклад, у методі Дельфі. Зазвичай для збіжності думок експертів достатньо трьох турів за умови чіткого розуміння ними цілей оцінювання. Важливим є також визначення чисельності експертної групи: занадто мала група знижує надійність результатів, тоді як велика група ускладнює організацію роботи та забезпечення кваліфікації всіх учасників.

Кількість експертів у групі обчислюють за виразом:

$$Q = \left[\beta t_{p,k-1} / \alpha\right]^2, \tag{2.3}$$

де Q – кількість експертів; β – варіація (показник достовірності проведеної експертизи); $t_{p,k-1}$ – коефіцієнт Стьюдента; α – відносна величина довірчого інтервалу.

Варіація визначається як:

$$\beta = \sigma / \bar{x}, \tag{2.4}$$

де σ – середньоквадратичне відхилення експертних оцінок; $\bar{x}$ – середнє значення оцінок.

Відносну ширину довірчого інтервалу визначають за формулою:

$$\alpha = \Delta x / \bar{x}, \tag{2.5}$$

де Δx – довірчий інтервал оцінки.

Найбільш простий підхід до групової оцінки полягає у використанні середнього балу:

$$x_i = \frac{1}{n}\sum_{j=1}^{n} x_{ij} \ , \tag{2.6}$$

де x_{ij} – оцінка i-го об'єкта j-м експертом.

Цей вираз передбачає, що усереднення оцінок здійснюється за умов рівноправності всіх експертів, тобто кожен внесок враховується з однаковим коефіцієнтом $1/n$. Щоб відобразити реальну «нерівність» експертів, що виникає через відмінності в компетентності, об’єктивності та інформованості, вводять вагові коефіцієнти, що відображають рівень компетентності кожного експерта [19].

3 МЕТОД АНАЛІЗА ІЄРАРХІЙ І МЕТОД ЕКСПЕРТНОГО ОЦІНЮВАННЯ ДЛЯ ВИБОРУ ПЕРЕВАЖНОГО ПРОТОКОЛУ МАРШРУТИЗАЦІЇ БЕЗДРОТОВИХ СЕНСОРНО-АКТУАТОРНИХ МЕРЕЖ

Розглядаються особливості використання методу аналізу ієрархій для визначення найбільш доцільного варіанту протоколу маршрутизації з урахуванням сукупності показників якості. Як критерії оцінювання обрано ключові технічні характеристики протоколів маршрутизації, зокрема мобільність, енергоспоживання, узгодженість, агрегацію даних, локалізацію, підтримку QoS, складність структури, масштабованість та наявність множинних маршрутів. У табл. 1.1 наведено характеристики показників якості для одинадцяти різних протоколів маршрутизації. На рис. 3.1 показано ієрархічне представлення завдання вибору переважного протоколу маршрутизації [1].

У табл. 3.2 показано матрицю парних порівнянь протоколів маршрутизації, сформовану експертом №1 на основі даних таблиці 3.1 відповідно до виразу (2.1). Далі обчислено власний вектор та вектор пріоритетів згідно за виразом (2.2). Для всіх матриць значення відношення узгодженості перебуває в допустимих межах. Аналогічним чином побудовано матриці парних порівнянь експертами №2–№10, наведені в таблицях 3.3–3.11.

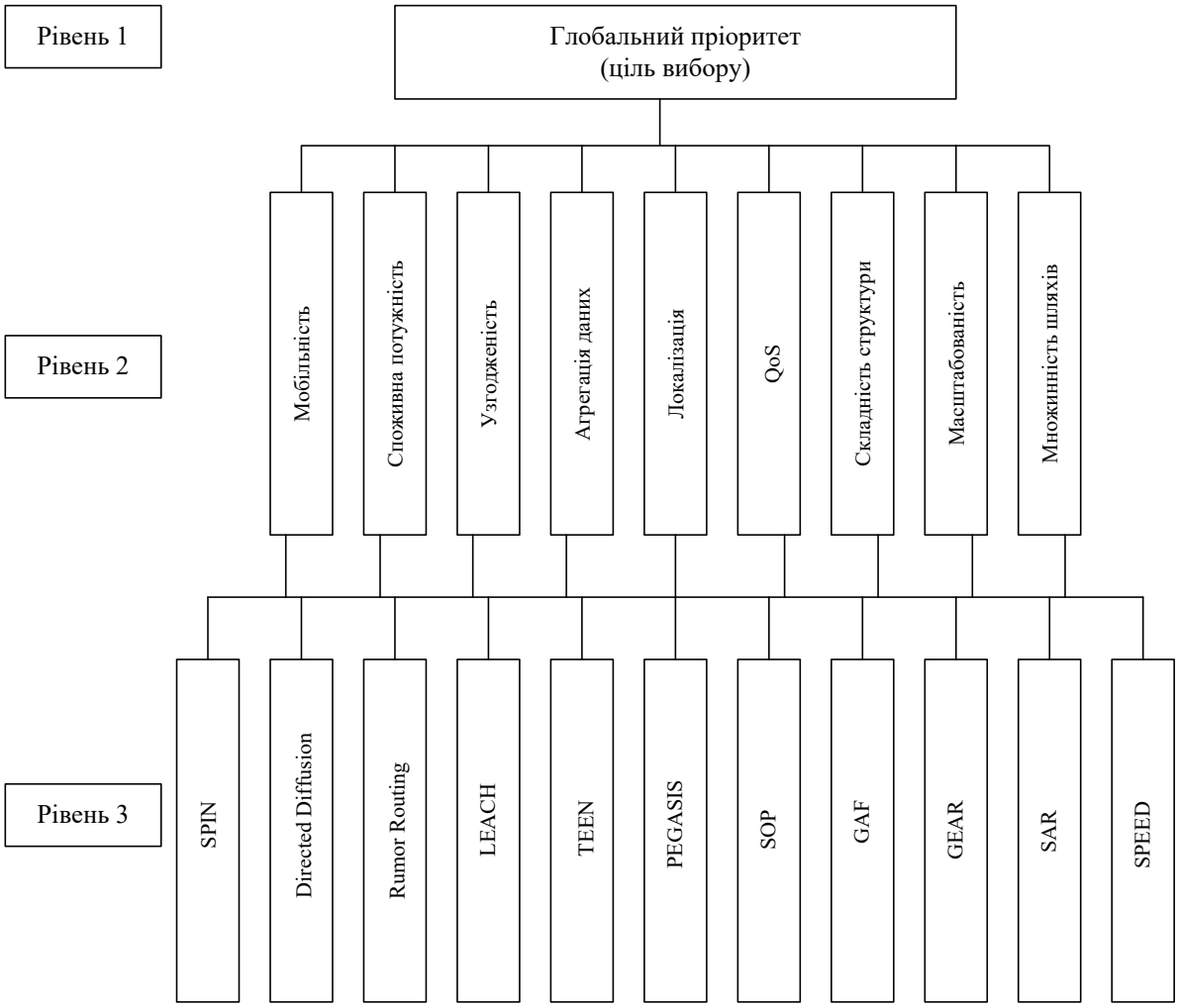

Рисунок 3.1 – Ієрархічна декомпозиція задачі вибору протоколів маршрутизації

Таблиця 3.2 – Складена матриця попарних порівнянь протоколів маршрутизації за оцінками експерта 1

№1	N1	N2	N3	N4	N5	N6	N7	N8	N9	N10	N11	V_1	P_1
N1	1	1/3	1/2	1/5	1/6	3	2	1/7	1/9	4	5	0,661	0,038
N2	3	1	2	1/2	1/4	4	3	1/5	1/6	6	7	1,258	0,073
N3	2	1/2	1	1/3	1/4	5	3	1/6	1/7	5	6	0,988	0,057
N4	5	2	3	1	1/2	5	4	1/3	1/4	6	7	1,88	0,109
N5	6	4	4	2	1	6	5	1/2	1/3	5	6	2,543	0,148
N6	1/3	1/4	1/5	1/5	1/6	1	1/2	1/5	1/8	2	3	0,399	0,023
N7	1/2	1/3	1/3	1/4	1/5	2	1	1/6	1/7	3	4	0,555	0,031

Продовження таблиці 3.2

N8	7	5	6	3	2	5	6	1	1/2	7	8	3,529	0,205
N9	9	6	7	4	3	8	7	2	1	8	9	4,87	0,283
N10	1/4	1/6	1/5	1/6	1/5	1/2	1/3	1/7	1/8	1	2	0,297	0,018
N11	1/5	1/7	1/6	1/7	1/6	1/3	1/4	1/8	1/9	1/2	1	0,222	0,0129

Таблиця 3.3 – Складена матриця попарних порівнянь протоколів маршрутизації за оцінками експерта 2

№2	№1	№2	№3	№4	№5	№6	№7	№8	№9	№10	№11	V_2	P_2
N1	1	1/4	2	1/3	1/4	3	2	1/7	1/8	5	6	0,832	0,047
N2	4	1	3	1/3	1/4	5	4	1/5	1/6	6	7	1,352	0,0768
N3	1/2	1/3	1	1/3	1/5	4	3	1/4	1/5	5	6	0,862	0,049
N4	3	3	3	1	1/3	6	5	1/3	1/4	7	8	1,91	0,108
N5	4	4	5	3	1	7	6	1/2	1/3	7	8	2,829	0,1608
N6	1/3	1/5	1/4	1/6	1/7	1	1/3	1/7	1/8	2	3	0,366	0,0208
N7	1/2	1/4	1/3	1/5	1/6	3	1	1/7	1/8	4	5	0,552	0,031
N8	7	5	4	3	2	7	7	1	1/3	8	9	3,504	0,199
N9	8	6	5	4	3	8	8	3	1	8	9	4,908	0,279
N10	1/5	1/6	1/5	1/7	1/7	1/2	1/4	1/8	1/8	1	2	0,268	0,016
N11	1/6	1/7	1/6	1/8	1/8	1/3	1/5	1/9	1/9	1/2	1	0,203	0,012

Таблиця 3.4 – Складена матриця попарних порівнянь протоколів маршрутизації за оцінками експерта 3

№3	№1	№2	№3	№4	№5	№6	№7	№8	№9	№10	№11	V_3	P_3
N1	1	1/2	2	1/4	1/6	3	2	1/8	1/9	4	5	0,784	0,0503
N2	2	1	2	1/3	1/3	2	2	1/3	1/5	6	7	1,155	0,074
N3	1/2	1/2	1	1/2	1/3	3	2	1/4	1/6	4	5	0,865	0,055
N4	4	3	2	1	2	5	4	1/2	1/3	4	4	2,039	0,1308

Продовження таблиці 3.4

N5	1/6	3	3	1/2	1	5	4	1/2	1/3	6	6	1,503	0,096
N6	1/3	1/2	1/3	1/5	1/5	1	2	1/7	1/9	2	3	0,492	0,0315
N7	1/2	1/2	1/2	1/4	1/4	1/2	1	1/6	1/7	2	3	0,505	0,0324
N8	8	3	4	2	2	7	6	1	2	7	8	3,705	0,2377
N9	9	5	6	3	3	9	7	1/2	1	7	7	3,959	0,255
N10	1/4	1/6	1/4	1/4	1/6	1/2	1/2	1/7	1/7	1	2	0,325	0,0208
N11	1/5	1/7	1/5	1/4	1/6	1/3	1/3	1/8	1/7	1/2	1	0,249	0,0159

Таблиця 3.5 – Складена матриця попарних порівнянь протоколів маршрутизації за оцінками експерта 4

№4	№1	№2	№3	№4	№5	№6	№7	№8	№9	№10	№11	V_4	P_4
N1	1	1/3	1/2	1/3	1/3	2	2	1/6	1/7	3	4	0,729	0,045
N2	3	1	2	1/2	1/3	4	3	1/3	1/5	5	6	1,332	0,0825
N3	2	1/2	1	1/3	1/3	3	2	1/4	1/6	4	5	0,947	0,0586
N4	3	2	3	1	1/2	5	4	1/3	1/4	1/5	1/6	0,937	0,0586
N5	3	3	3	2	1	7	6	1/2	1/3	7	8	2,472	0,1532
N6	1/3	1/4	1/3	1/5	1/7	1	1/2	1/7	1/9	2	3	0,396	0,0245
N7	1/2	1/3	1/2	1/4	1/6	2	1	1/6	1/8	3	3	0,546	0,0338
N8	6	3	4	3	2	7	6	1	1/2	7	8	3,301	0,2045
N9	7	5	6	4	3	9	8	2	1	8	9	4,723	0,2927
N10	1/3	1/5	1/4	5	1/7	1/2	1/3	1/7	1/8	1	2	0,419	0,0259
N11	1/4	1/6	1/5	6	1/8	1/3	1/3	1/8	1/9	1/2	1	0,332	0,0205

Таблиця 3.6 – Складена матриця попарних порівнянь протоколів маршрутизації за оцінками експерта 5

№5	№1	№2	№3	№4	№5	№6	№7	№8	№9	№10	№11	V_5	P_5
N1	1	1/2	1/2	1/3	1/4	3	2	1/6	1/7	4	5	0,772	0,045

Продовження таблиці 3.6

N2	2	1	2	1/3	1/4	4	3	1/3	1/5	5	7	1,222	0,072
N3	2	1/2	1	1/3	1/4	4	3	1/4	1/5	4	5	0,999	0,059
N4	3	3	3	1	1/2	5	4	1/2	1/3	6	7	1,98	0,117
N5	4	4	4	2	1	6	5	1/2	1/3	7	8	2,592	0,153
N6	1/3	1/4	1/4	1/5	1/6	1	1/2	1/8	1/9	2	3	0,386	0,022
N7	1/2	1/3	1/3	1/4	1/5	2	1	1/7	1/8	3	4	0,541	0,0319
N8	6	3	4	2	2	8	7	1	1/2	8	9	3,341	0,198
N9	7	5	5	3	3	9	8	2	1	9	9	4,57	0,27
N10	1/4	1/5	1/4	1/6	1/7	1/2	1/3	1/8	1/9	1	2	0,293	0,076
N11	1/5	1/7	1/5	1/7	1/8	1/3	1/4	1/9	1/9	1/2	1	0,217	0,0128

Таблиця 3.7 – Складена матриця попарних порівнянь протоколів маршрутизації за оцінками експерта 6

№6	№1	№2	№3	№4	№5	№6	№7	№8	№9	№10	№11	V_6	P_6
N1	1	1/3	1/2	1/4	1/5	3	2	1/6	1/7	4	5	0,71	0,041
N2	3	1	2	1/2	1/3	5	4	1/3	1/5	6	7	1,439	0,084
N3	2	1/2	1	1/3	1/4	4	3	1/5	1/6	5	6	0,998	0,058
N4	4	2	3	1	1/2	5	4	1/3	1/4	6	7	1,842	0,107
N5	5	3	4	2	1	6	5	1/2	1/3	7	8	2,567	0,15
N6	1/3	1/5	1/4	1/5	1/6	1	1/2	1/7	1/8	2	3	0,387	0,022
N7	1/2	1/4	1/3	1/4	1/5	2	1	1/7	1/8	2	3	0,495	0,028
N8	6	3	5	3	2	7	7	1	1/2	7	8	3,416	0,199
N9	7	5	6	4	3	8	8	2	1	9	9	4,723	0,276
N10	1/4	1/6	1/5	1/6	1/7	1/2	1/2	1/7	1/9	1	1/2	0,261	0,0152
N11	1/5	1/7	1/6	1/7	1/8	1/3	1/3	1/8	1/9	2	1	0,251	0,0146

Таблиця 3.8 – Складена матриця попарних порівнянь протоколів маршрутизації за оцінками експерта 7

№7	№1	№2	№3	№4	№5	№6	№7	№8	№9	№10	№11	V_7	P_7
N1	1	1/3	1/2	1/4	1/5	2	3	1/7	1/7	5	4	0,7	0,039
N2	3	1	2	1/2	1/3	4	5	1/5	1/5	7	6	1,375	0,076
N3	2	1/2	1	1/3	1/4	4	5	1/6	1/6	7	7	1,075	0,059
N4	4	2	3	1	1/2	5	6	1/4	1/4	8	7	1,913	0,106
N5	5	3	4	2	1	6	7	1/2	1/3	9	8	2,718	0,151
N6	1/2	1/4	1/4	1/5	1/6	1	2	1/8	1/8	4	3	0,489	0,027
N7	1/3	1/5	1/5	1/6	1/7	1/2	1	1/9	1/9	3	2	0,355	0,019
N8	7	5	6	4	2	8	9	1	1/2	9	9	4,056	0,226
N9	7	5	6	4	3	8	9	2	1	9	9	4,774	0,266
N10	1/4	1/7	1/7	1/8	1/9	1/4	1/3	1/9	1/9	1	1/2	0,21	0,012
N11	1/5	1/6	1/7	1/7	1/8	1/3	1/2	1/9	1/9	2	1	0,258	0,014

Таблиця 3.9 – Складена матриця попарних порівнянь протоколів маршрутизації за оцінками експерта 8

№8	№1	№2	№3	№4	№5	№6	№7	№8	№9	№10	№11	V_8	P_8
N1	1	1/2	1/3	1/4	1/5	3	2	1/6	1/7	5	4	0,71	0,041
N2	2	1	1/2	1/3	1/4	4	3	1/5	1/6	7	6	1,029	0,059
N3	3	2	1	1/2	1/3	5	4	1/4	1/5	7	6	1,403	0,081
N4	4	3	2	1	1/2	6	5	1/3	1/4	8	7	1,96	0,113
N5	5	4	3	2	1	7	6	1/2	1/3	9	8	2,718	0,157
N6	1/3	1/4	1/5	1/6	1/7	1	1/2	1/8	1/9	3	2	0,367	0,021
N7	1/2	1/3	1/4	1/5	1/6	2	1	1/7	1/8	3	3	0,495	0,029
N8	6	5	4	3	2	8	7	1	1/2	8	7	3,55	0,204
N9	7	6	5	4	3	9	8	2	1	8	7	4,6169	0,266
N10	1/5	1/7	1/7	1/8	1/9	1/3	1/3	1/8	1/8	1	1/2	0,2163	0,012
N11	1/4	1/6	1/6	1/7	1/8	1/2	1/3	1/7	1/7	2	1	0,28	0,016

Таблиця 3.10 – Складена матриця попарних порівнянь протоколів маршрутизації за оцінками експерта 9

№9	№1	№2	№3	№4	№5	№6	№7	№8	№9	№10	№11	V_9	P_9
N1	1	1/3	1/2	1/5	1/4	3	2	1/6	1/7	4	5	0,711	0,042
N2	3	1	2	1/3	1/2	6	5	1/3	1/5	7	8	1,533	0,09
N3	2	1/2	1	1/3	1/2	4	3	1/4	1/5	6	7	1,138	0,066
N4	5	3	3	1	2	6	5	1/2	1/3	7	8	2,51	0,147
N5	4	2	2	1/2	1	5	4	1/3	1/4	6	7	1,775	0,104
N6	1/3	1/6	1/4	1/6	1/5	1	1/2	1/7	1/8	2	3	0,381	0,022
N7	1/2	1/5	1/3	1/5	1/4	2	1	1/6	1/7	3	4	0,531	0,031
N8	6	3	4	2	3	7	6	1	1/2	8	9	3,377	0,199
N9	7	5	5	3	4	8	7	2	1	9	9	4,589	0,269
N10	1/4	1/7	1/6	1/7	1/6	1/2	1/3	1/8	1/9	1	2	0,273	0,017
N11	1/5	1/8	1/7	1/8	1/7	1/3	1/4	1/9	1/9	1/2	1	0,208	0,0128

Таблиця 3.11 – Складена матриця попарних порівнянь протоколів маршрутизації за оцінками експерта 10

№10	№1	№2	№3	№4	№5	№6	№7	№8	№9	№10	№11	V_{10}	P_{10}
N1	1	1/2	2	1/3	1/4	3	2	1/5	1/6	4	5	0,904	0,054
N2	2	1	3	1/2	1/3	5	4	1/3	1/4	5	6	1,424	0,0849
N3	1/2	1/3	1	1/3	1/4	3	2	1/5	1/6	4	5	0,767	0,046
N4	3	2	3	1	1/2	5	4	1/3	1/3	6	6	1,815	0,108
N5	4	3	4	2	1	6	6	1/2	1/3	7	8	2,56	0,153
N6	1/3	1/5	1/3	1/5	1/6	1	1/2	1/7	1/8	2	3	0,397	0,024
N7	1/2	1/4	1/2	1/4	1/6	2	1	1/7	1/8	3	3	0,524	0,031
N8	5	3	5	3	2	7	7	1	1/2	8	8	3,402	0,203
N9	6	4	6	3	3	8	8	2	1	9	9	4,446	0,265
N10	1/4	1/5	1/4	1/6	1/7	1/2	1/3	1/8	1/9	1	2	0,293	0,017
N11	1/5	1/6	1/5	1/6	1/8	1/3	1/3	1/8	1/9	1/2	1	0,232	0,014

У табл. 3.12 наведено результати обробки оцінок матриць парних порівнянь, отриманих від десяти експертів, а також відповідні вектори пріоритетів, обчислені згідно з формулою (2.2). На їх основі визначено середній вектор пріоритетів відповідно до виразу (2.6). Представлено вибір переважного варіанта протоколу маршрутизації з урахуванням експертних суджень на основі методу аналізу ієрархій.

Таблиця 3.12 – Вибір протоколу маршрутизації БСАМ за методом експертного оцінювання

Протоколи	Оцінки парних порівнянь 10 експертів (P_j)										Середня оцінка вектора пріоритетів 10 експертів
	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	
N1	0,03	0,04	0,05	0,04	0,04	0,04	0,03	0,04	0,04	0,05	0,0442
N2	0,07	0,07	0,07	0,08	0,07	0,08	0,07	0,05	0,09	0,08	0,077
N3	0,05	0,04	0,05	0,05	0,05	0,05	0,05	0,08	0,06	0,04	0,0589
N4	0,10	0,10	0,13	0,05	0,11	0,1	0,1	0,11	0,14	0,10	0,1103
N5	0,14	0,16	0,09	0,15	0,15	0,15	0,15	0,15	0,10	0,15	0,1426
N6	0,02	0,02	0,03	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,0237
N7	0,03	0,03	0,03	0,03	0,03	0,02	0,01	0,02	0,03	0,03	0,0299
N8	0,20	0,19	0,23	0,2	0,19	0,19	0,22	0,2	0,19	0,20	0,2076
N9	0,28	0,27	0,25	0,29	0,27	0,27	0,26	0,26	0,26	0,26	0,2721
N10	0,01	0,01	0,02	0,02	0,07	0,01	0,01	0,01	0,01	0,01	0,023
N11	0,01	0,01	0,01	0,02	0,01	0,01	0,01	0,01	0,01	0,01	0,0145

З аналізу даних табл. 3.12 бачимо, що відповідно до методів знаходженн переважного варіанта доцільно обрати протокол маршрутизації N9 – GEAR, оскільки він характеризується максимальним значенням компоненти вектора пріоритетів [1].

ВИСНОВОК

У даній роботі розглянуто метод аналізу ієрархій і метод експертного оцінювання. Досліджено можливості їх застосування для визначення пріоритетного протоколу маршрутизації на основі експертних суджень щодо характеристик методів маршрутизації в бездротових сенсорно-актуаторних мережах.

За результатами проведеного вибору встановлено, що протокол GEAR демонструє найвищу ефективність для використання в польових БСАМ із відомим розташуванням елементів мережі.

Отримані результати з використанням методу аналізу ієрархій та методу експертного оцінювання підтверджують доцільність застосування цих підходів під час проєктування бездротових сенсорно-актуаторних мереж. Перевагою запропонованого підходу є відмова від традиційного «інтуїтивного» вибору, за якого рішення приймалося експертом виключно на основі власного досвіду та окремих параметрів мережі. Натомість використання формалізованих методів дозволяє знизити ймовірність помилкових рішень завдяки обробці узагальнених даних від кількох експертів із застосуванням строгого математичного апарату.

Метод аналізу ієрархій та метод експертного оцінювання можуть бути також ефективно використані для оцінювання та вибору рішень у межах інших телекомунікаційних технологій і апаратних платформ.

ПЕРЕЛІК ПОСИЛАНЬ

1. Bezruk V., Zelenin A., Vlasova V., Skorik J., Koltun Y. Select preferred of wireless sensor and actuator network // Eastern European Journal of Enterprise Technologies, 1/9 (79). – 2016. – P.4-9.
2. Heinzelman W., Kulik J., Balakrishnan H. Adaptive Protocols for Information Dissemination in Wireless Sensor Networks / Proc. 5th ACM/IEEE Mobicom Conference (MobiCom ’99), Seattle, WA. – 1999. – P. 174-85.
3. Intanagonwiwat C., Govindan R., Estrin D. Directed diffusion: a scalable and robust communication paradigm for sensor networks / Proceedings of ACM MobiCom’00, Boston, MA. – 2000.– P. 56-67.
4. Feng Zhao, Leonidas J. Guibas. Wireless Sensor Networks. – 2004. – P.63-102. DOI: 10.1016/B978-155860914-3/50003-1.
5. Braginsky D., Estrin D. Rumor Routing Algorithm For Sensor Networks / International Conference on Distributed Computing Systems (ICDCS’01), November 2001.
6. Jun Zheng. Wireless sensor networks a Networking Perspective. John Wiley & Sons, Inc., Hoboken, New Jersey. – 2009. ISBN: 978-0-470-16763-2.
7. Heinzelman W., Chandrakasan A., Balakrishnan H. Energy-Efficient Communication Protocol for Wireless Microsensor Networks / Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS ’00), January, 2000.
8. Manjeshwar A., Agarwal D.P. TEEN: a routing protocol for enhanced efficiency in wireless sensor networks / 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, April, 2001.
9. Lindsey S., Raghavendra C. PEGASIS: Power-Efficient Gathering in Sensor Information Systems / IEEE Aerospace Conference Proceedings. – 2002. – Vol. 3. – P. 1125-1130.

10. Sohrabi K., Pottie J. Protocols for self-organization of a wireless sensor network / IEEE Personal Communications. – 2000. – Vol. 7. – №5. – P. 16-27.
11. M. C. Vuran and O. B. Akan. Spatio - temporal characteristics of point and field sources in wireless sensor networks / In Proceedings of IEEE ICC' 06, Istanbul, Turkey, June 2006. – P. 234-239.
12. Y. Fang and B. McDonald , " Dynamic codeword routing (DCR): A cross – layer approach for performance enhancement of general multi-hop wireless routing ", in Proceedings of IEEE SECON ' 04, Santa Clara, CA, Oct. 2004. – P. 255-263.
13. He T. SPEED: A stateless protocol for real-time communication in sensor networks / Proceedings of International Conference on Distributed Computing Systems, Providence, RI, May 2003.
14. Yu Y., Heidemann J., Estrin D. Geography-informed Energy Conservation for Ad-hoc Routing / In Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking. – 2001. – P. 70-84.
15. Yu Y., Estrin D., R. Govindan Geographical and Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks / UCLA Computer Science Department Technical Report, UCLA-CSD TR-01-0023, May 2001.
16. Иваненко В. Анализ протоколов передачи данных от узлов в беспроводных сенсорных сетях / Восточно-Европейский журнал передовых технологий. – 2011. – Т. 2, N 10(50). – С. 9-12. – Режим доступа: DOI: 10.15587/1729-4061.2011.1860.
17. Saaty T.L. The analytic hierarchy and analytic network measurement processes: applications to decisions under risk. European journal of pure and applied mathematics 1 (1). – 2008. – P. 122-196.
18. Saaty T.L. The Analytic Hierarchy Process, New York: McGraw Hill. – 1980.
19. Безрук В.М., Скорик Ю.В. Выбор оптимальных речевых кодеков методами экспертного оценивания / Восточно-Европейский журнал передовых технологий. – Харків. – 2012. – 3/2 (57). – С. 19-24.