УДК 621.311

О.Тимченко[1)] , М.Зеляновський [2)]

АНАЛІЗ ХАРАКТЕРИСТИК ІЄРАРХІЧНИХ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

Розглядаються характеристики популярних «ієрархічних» протоколів маршрутизації безпровідних сенсорних мереж, в яких вузли групуються за досяжністю в кластери, центри яких в основному приймають участь в маршрутизації повідомлень. Аналізуються існуючі протоколи обміну даних та час функціонування мережі.

Ключові слова: сенсорні мережі, енергозбереження, комунікаційні протоколи.

Descriptions of popular «hierarchical» protocols of routing of off-wire sensory networks, in which knots form a group after reach in clusters the centers of which mainly take part in routing of messages, are examined. Existent protocols of exchange of information and time of functioning of network are analysed.

Keywords: sensory networks, energy effective, communication protocols.

Вступ

В безпровідних сенсорних мережах протоколи маршрутизації прийнято ділити на однорідні або ієрархічні [1]. Однорідні структури інтерпретують всі вузли однаковими і вони рівномірно беруть участь в процесі маршрутизації. Проте це викликає швидке і нерівномірне вичерпання енергетичних ресурсів сенсора. Для подолання цього недоліку розроблені «ієрархічні» протоколи маршрутизації в безпровідних сенсорних мережах, в яких вузли групуються за досяжністю чи іншими критеріями в кластери, центри яких (головні вузли) в основному приймають участь в маршрутизації повідомлень (рис.1).

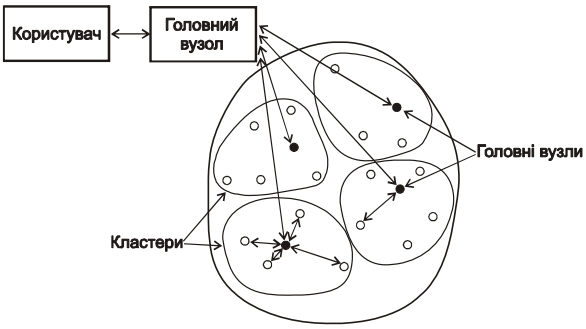

Рис.1. Принцип функціонування однорідних протоколів маршрутизації

[1] Українська академія друкарства
[2] Національний університет „Львівська політехніка”

Метою роботи є аналіз популярних протоколів однорідної маршрутизації та їх можливості для забезпечення функціональності мережі та максимально можливого часу її дії.

Характеристики ієрархічнних протоколів маршрутизації

Протокол LEACH (*Low-Energy Adaptive Clustering Hierarchy*) [2], [3] або низькоенергетична адаптивна ієрархія груп (кластерів) є одним з перших ієрархічних протоколів маршрутизації в сенсорних мережах. Це протокол, що базується на кластерному формуванні вузлів сенсорних мереж, які служать для комунікації з головним вузлом (*sink*). В протоколі використано випадкову зміну головних вузлів в кластерах, що дозволило зменшити використання енергії і рівномірно розподілити енергетичне навантаження на всі вузли в мережі. LEACH використовує рівномірну локалізацію для забезпечення масштабованості сенсорних мереж, а також виконує агрегацію даних, завдяки чому значно обмежує число даних, які транслюються до головного вузла. Крім того автори використали технології *TDMA (Time Division Multiplexing Access*) і *CDMA (Code Division Multipexing Access*), щоб зменшити міжкластерні і внутрікластерні колізії і інтерференції.

Функціонування протоколу LEACH можна поділити на дві фази: фазу організації і встановлену (робочу) фазу. У фазі організації організуються кластери і вибирається головний вузол в кожному кластері. У встановленій фазі виконується трансмісія даних до головного вузла в мережі. Встановлена фаза триває значно довше за фазу організації, що витікає з бажання мінімізувати додаткові втрати в мережі, а також ефектно її використовувати.

Під час фази організації деяка частина мережевих вузлів p вибирає з поміж себе головний вузол, за допомогою представленого нижче алгоритму:

- сенсорний вузол вибирає випадкове число r з проміжку від 0 до 1. Якщо це число менше ніж задана порогова вартість $T(n)$, то вузол стає головним вузлом для даного кластеру.
- порогова вартість розраховується за формулою (1), в якій використовується «бажання вузла» стати головним вузлом для кластеру (значення r), в теперішньому періоді вибору, а також групи вузлів ще не вибраних як головним в останніх $1/p$ періодах – позначених як G:

$$T(n) = \frac{p}{1 - p(r \cdot \mathrm{mod}(1/p))} \quad якщо\ n \in G. \tag{1}$$

Після того як головні вузли були вибрані, вони розсилають до всіх інших вузлів інформацію про своє існування. Під час прийому цієї інформації вузли вирішують, до яких кластерів хочуть належати. При цьому виборі головною метрикою є потужність сигналу при прийомі сигналу від головного вузла. Надалі сенсорні вузли інформують вибрані головні вузли, що будуть членами їх кластера. Цей процес надзвичайно важливий, оскільки при невеликому комунікаційному радіусі частина вузлів взагалі не приєднається до жодного кластера.

Після отримання всієї інформації від вузлів, які хочуть входити до складу кластера, головний вузол призначає кожному вузлу часовий інтервал згідно технології TDMA, щоб той міг транслювати до нього дані. Під час встановленої фази вузли в кластері можуть виконувати свої завдання (вимірювання і спостереження) і транслювати дані в своєму часовому інтервалі. Головний вузол агрегує дані, отримані від вузлів в кластері і пересилає їх до головного вузла. Після визначеного часу мережа повертається до фази організації і виконує наступний період обрання головних вузлів для кластерів (рис.2). Слід зазначити, що кожен кластер використовує різні коди CDMA під час комунікації, що зменшує інтерференцію від вузлів, що належать до інших кластерів.

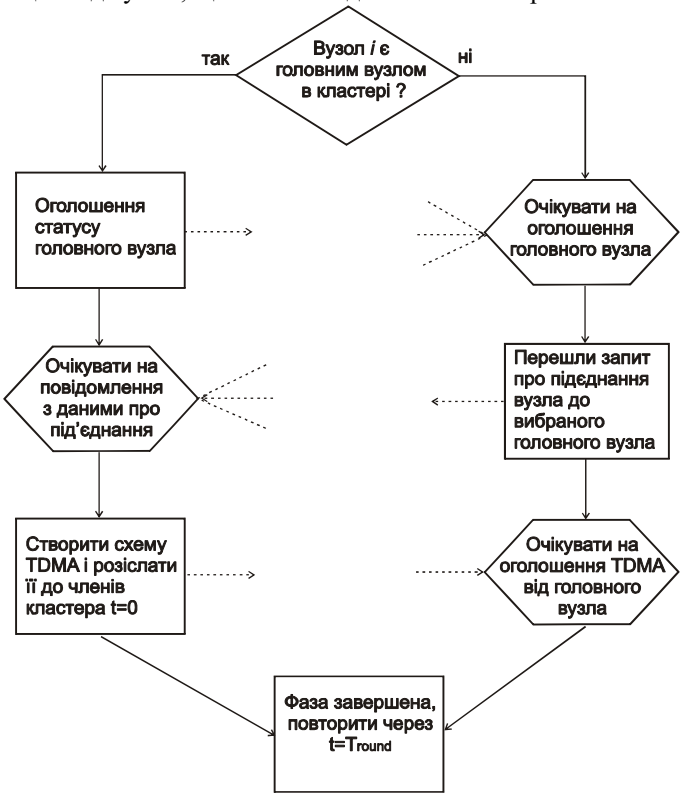

Рис. 2. Послідовність вибору головних вузлів в протоколі LEACH

Очевидно, що використання протоколу LEACH дозволяє підняти живучість мережі. Проте існують певні недоліки протоколу:

- він базується на тому, що кожен вузол в мережі має енергію, що вимагається для трансмісії даних і, забезпечує енергією протоколи нижчих рівнів, що може бути помилкою.

- не передбачає ситуації, в якій вузли лежать дуже близько між собою і транслюють ідентичні дані.
- приймає, що вузли весь час мають дані для висилання.
- важко визначити чи передбачити необхідне число головних вузлів кластерів *p.* Можлива ситуація при якій вибрані головні вузли лежать в тій самі частини мережі, а деякі вузли можуть не належати до жодних кластерів.

Через вказані причини протокол вимагає певних покращень. Одним з найважливіших є створення механізму, який враховує неоднорідні енергетичні ресурси кожного вузла. Іншим є додавання до протоколу фази переговорів, які подібно як в протоколі SPIN, вирішували чи необхідно пересилати дані від вузлів в кластерах до головних вузлів. Це може забезпечити пересилання тільки нової інформації до головного вузла, а значить зменшити споживання енергії.

Протокол TEEN *(Threshold sensitive Energy Efficient sensor Network)* [4] є ієрархічним протоколом, на основі добре відомого протоколу LEACH. Протокол застосовує реактивну маршрутизацію і призначений для застосувань, в яких важливим є невідкладний вияв значних змін величини вимірюваного параметру, наприклад, температури.

Подібно як в протоколі LEACH сенсорні вузли організовані в кластери і вибирається головний вузол кластеру. Далі головний вузол розсилає дві величини порогу до всіх вузлів: твердий (мінімальний) поріг H_T (*hard threshold*) і м'який поріг S_T (*soft threshold*), а також призначає часовий інтервал в TDMA. Твердий поріг - це мінімальна величина вимірюваного параметру, при якому наступає включення передавача і трансляція даних до головного вузла. Завдяки цьому твердий поріг дозволяє трансмісію вузлу тільки якщо параметр має необхідність, а тому зменшує число трансмісії.

Вузол записує виміряну величину (вищу від H_T) в змінну, що називається CV (*sesned value*). Наступні дані вузол транслюватиме, якщо будуть виконані дві умови:

- наступна виміряна величина параметру є вища від твердого порогу H_T
- наступна виміряна величина параметру відрізняється від попередньої виміряної величини CV на величину більшу або рівну м'якому порогу S_T.

Як результат м'який поріг зменшує число трансмісії, якщо немає відповідної зміни виміряного параметру або вона мінімальна, завдяки чому сприяє меншому споживанню енергії. Відповідне встановлення м'якого і твердого порогу дає можливість регулювати число трансльованих пакетів.

Головною вадою протоколу є те, що якщо вказані пороги не будуть досягнуті, то вузол ніколи не зв'яжеться з головним вузлом і користувач не отримає жодних даних з мережі. Якщо інтерполювати цю ситуацію, то користувач може навіть не знати, що всі вузли в мережі були знищені. Крім того протокол може витрачати часові інтервали, призначені для вузів, які нічого не транслюють. З цих же причин протокол не відповідає вимогам

застосувань, де дані мусять передаватись регулярно. Тому вважається, що найкращим застосуванням протоколу TEEN є виявлення особливих подій, наприклад, вибуху чи пожежі.

Протокол APTEEN *(**A**daptive **T**hreshold sensitive **E**nergy **E**fficient sensor Network)* [2] є розширенням протоколу TEEN і зосереджується однаковою мірою на перетворенні періоду даних з вузлів так і на реакції на виявлення (*event-driven*), застосовує гібридну маршрутизацію. Протокол подібно до протоколу TEEN встановлює твердий і м'який пороги, а також призначає часовий інтервал для кожного вузла згідно технології TDMA. Крім того був введений лічильник часу CT (*count time*), який визначає максимальний час між пересиланням наступних рапортів даних. Потрібно зазначити, що APTEEN дозволяє застосування трьох різних запитів: «історичний» – аналіз даних з минулого, «дійсний» – аналіз актуального стану мережі і «моніторинг» – нагадування про необхідність вимірювання і передачу через визначений період часу в майбутньому. На відміну від протоколу TEEN розрізняє пошкоджені вузли в мережі, а також більш гнучко і оптимально призначає часові інтервали.

Проте протокол має більшість недоліків протоколу LEACH, а крім того більш складний.

Протокол PEGASIS *(Power-Efficient Gathering in Sensor Information Systems)* [4] є розширенням протоколу LEACH. Головною ідеєю протоколу є продовження життя мережі шляхом комунікації вибраного вузла тільки з найближчим сусідом, а також періодичний вибір вузла, який підтримуватиме зв'язок з головним вузлом. Коли період роботи всіх вузлів, що підтримують зв'язок з головним вузлом закінчиться, наступає початок наступного періоду вибору головного вузла і т.д. Така періодична зміна функцій вузлів значно зменшує енергію, необхідну для трансмісії даних під час періоду роботи, тому що замовлення на передачу даних рівномірно розкладається на всі вузли. Завдяки цьому протокол досягає двох завдань:

- збільшує тривалість життя кожного вузла шляхом використання співпраці сусідніх вузлів, а тим самим збільшує життя всієї мережі
- дозволяє тільки місцеву координацію між найближчими вузлами, завдяки чому значно зменшене використання смуги при комунікації.

Щоб локалізувати найближчого сусіда кожен вузол використовує значення потужності прийнятого сигналу в залежності від віддаленості до сусідніх вузлів, а далі підстроює потужність сигналу так, щоб він отримувався тільки одним вузлом. Коло, створюване PEGASIS, складається з найближчих вузлів, в результаті чого формується шлях до головного вузла. Загреговані дані пересилається через кожен вузол в колі, а вузли в наступних періодах визначають, який з них стане головним і буде пересилати дані безпосередньо до головного вузла. Автори протоколу в своїх симуляціях [3]

показали, що PEGASIS може продовжити час життя мережі вдвічі в порівнянні з мережею, що функціонує за протоколом LEACH, – рис.3.

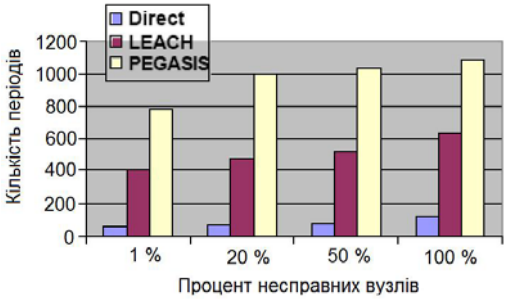

Рис. 3. Продовження часу життя мережі завдяки застосуванню протоколу PEGASIS в порівнянні з протоколом LEACH. Мережа займає простір 50м х 50м і має початкову енергію 25Дж/вузол

Проте протокол PEGASIS вимагає прийняття певних обмежень, що значно утрудняє його застосування в деяких застосуваннях:

- кожен вузол в мережі може підтримувати зв'язок з головним вузлом, а як відомо з практики, сенсорні вузли використовують багатокрокову комунікацію;
- кожен вузол в мережі отримує і керує повною базою даних про локалізацію всіх вузлів в мережі;
- всі вузли в мережі мають однакові енергетичні ресурси і імовірно загинуть одночасно.

З цих причин протокол PEGASIS може бути застосовуваний тільки в особливих застосуваннях.

Протокол HAR *(Hierarchy-based Anycast Routing)* [5, 6] це протокол маршрутизації, який будує дерево маршрутизації в головному вузлі. Цей вузол ініціює формування дерева маршрутизації шляхом розповсюдження пакету, запрошуючого інші вузли. Вузол, отримуючий пакет із запрошенням, чекає на інші такі пакети від альтернативних головних вузлів, а надалі вибирає найкращий з них і висилає пакет з бажанням під'єднатись. Головний вузол підтверджує відповідь вузла і пересилає пакет «схвалення». Якщо вузол не отримає пакету «схвалення» за визначений час, то висилає наступний пакет з бажанням під'єднання до головного вузла (другий і останній раз). Коли вузол отримає пакет «схвалення», він починає працювати на вибраний головний вузол разом з іншими вузлами і в свою чергу розсилає пакет із запрошенням. Таким способом створюється ієрархічна структура мережі, в якій кожен вузол („дитя") знає свій головний вузол („батька") і головний вузол („діда") свого головного вузла.

Оскільки вузол пересилає всі дані завжди тільки до головного вузла,

одним з головних недоліків протоколу є проблема „hotspot" або надмірне використання головних вузлів, що з часом приведе до їх зникнення. Крім того під час формування таблиці маршрутизації висилається дуже велике число пакетів, що вводить значний надлишок трансльованих даних.

Висновки

Переваги ієрархічних протоколів маршрутизації

- агрегація даних – в протоколах ієрархічної маршрутизації агрегація даних характеризується великою продуктивністю. Дані з окремих вузлів в кластері передаються до головного вузла і там агрегуються з подібними даними перед пересиланням до головного вузла.

Недоліки:

- проблема „hotspot" – вузол, вибраний як головний вузол кластера, витрачає більше енергії ніж інші вузли. Тому, якщо не наступає регулярна ротація головних вузлів, можуть вичерпатись його ресурси і відбутись ряд відсічень сенсорних просторів від мережі.
- енергетичні вимоги – багато ієрархічних протоколів маршрутизації вимагає, щоб вузли головного кластеру володіли більшими енергетичними ресурсами від інших вузлів мережі, тому що більше її споживають.
- складність – якщо вузол головного кластеру має однакові з іншими вузлами ресурси, то в протоколі обов'язково мусить передбачений метод селекції і ротації при виборі головного вузла кластера, щоб зрівноважити споживання енергії. Проте таке рішення вводить додаткові службові повідомлення і додатковий трафік.

Порівняння однорідних та ієрархічних протоколів

Різний підхід до маршрутизації даних в цих протоколах представлений в табл. 1.

Таблиця 1

Параметр порівняння	**Ієрархічна маршрутизація**	**Однорідна маршрутизація**
Доступ до середовища	Кожен вузол має призначений свій часовий слот	Доступ залежить від вмісту наявної інформації у вузлі
Колізії	Наступають	Не наступають
Коефіцієнт використання циклу роботи	Коефіцієнт використання циклу роботи зменшений завдяки фазі спання вузла.	Змінний коефіцієнт використання циклу роботи, контролюється часом присипання вузлів
Агрегація даних	Агрегація даних проводиться у головних вузлах	Вузол на багатокроковому шляху агрегує дані, що приходять від сусідніх вузлів

Алгоритм маршрутизація	Проста, але не оптимальна маршрутизація	Маршрутизація може стати оптимальною після додавання певних механізмів
Синхронізація	Вимагається глобальна і місцева синхронізація	З'єднання, створюються випадково, без синхронізації
Позатрансмісійний додаток	Додаткові витрати для формування кластерів у мережі	Шляхи, створюються тільки в регіонах з даними, готовими для трансмісії. Малі додаткові витрати
Затримка	Мала затримка розповсюдження, тому що мережа, створена на кластерах, завжди доступна	Затримка для вимоги „розбудження" непрямих вузлів, під час формування шляху до головного вузла
Використання енергії	Використання енергії однорідне і не може бути контрольоване	Використання енергії залежить від виду трафіку в мережі
Розподіл каналу	Справедливий розподіл каналу	Справедливий розподіл каналу не гарантований

Коротке порівняння протоколів, які найчастіше застосовуються в сенсорних мережах: SPIN, LEACH і Directed Diffusion, дано в табл. 2.

Таблиця 2

	SPIN	LEACH	Directed Diffusion
Оптимальний шлях	ні	ні	так
Час життя мережі	довгий	дуже довгий	довгий
Відомості про використання ресурсів	так	так	так
Використання вказівника «мета-дані»	так	ні	так

1. *Тимченко О.В., Зеляновський М.Ю.* Методи і протоколи обміну даними сенсорних мереж // Зб. наук. пр. ІПМЕ НАН України. – Вип.46. – К.: 2008. – С. 176-183.
2. *Ilyas M., Mahgoub I.* „*Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*", CRC Press, New York, 2005,
3. *Akkaya K., Younis M.* „A Survey on Routing Protocols for Wireless Sensor Networks", *Elsevier Ad Hoc Network Journal*, 2005 vol. 3, no.3, p. 325-349.
4. *Manjeshwar A., Agrawal D. P.* „TEEN : A Protocol for Enhanced Efficiency in Wireless Sensor Networks", *Proc. 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing*, San Francisco, USA, 2001,
5. *Braginsky D., Estron D.* „Rumor Routing Algorithm For Sensor Networks", *Proceedings of the first Workshop on Sensor Networks and Applications*, Atlanta, USA, 2002, p. 22–31.
6. *Thepvilojanapong N., Tobe Y., Sezaki K.* „HAR: Hierarchy-Based Anycast Routing Protocol for Wireless Sensor Networks," *Proceedings of the 2005.*

Поступила 2.08.2010р.