Обидва типи модифікацій без жодних застережень можна використати і стосовно кольорових зображень. Однак, незалежно від типу зображення, пропорційно до розмірності вхідного зображення може зростає розмір шифрованого зображення.

*1. Шнайер Б. Прикладная криптография. – М.: Триумф, 2003. – 815 с. 2. Яне Б. Цифровая обработка изображений. – М.: Техносфера , 2007. – 583 с. 3. Рашкевич Ю.М., Пелешко Д.Д., Ковальчук А.М., Пелешко М.З. Модифікація алгоритму RSA для деяких класів зображень // Технічні вісті 2008/1(27), 2(28). – С. 59–62. 4. Rashkevych Y., Kovalchuk A., Peleshko D., Kupchak M. Stream Modification of RSA Algorithm For Image Coding with precize contour extraction. Proceedings of the X-th International Conference CADSM 2009. 24–28 February 2009, Lviv–Polyana, Ukraine. – P. 469–473. 5. http://timara.con.oberlin.edu/~gnelson/mp3s/Long.mp3s.html*.

**УДК 681.3.06(075)**

**О. Кузьмін, О. Мицько, В. Грицак**
Національний університет “Львівська політехніка”,
кафедра автоматизованих систем управління

# КЛАСИФІКАЦІЯ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ У БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖАХ

*© Кузьмін О., Мицько О., Грицак В., 2010*

**Наведено класифікацію протоколів маршрутизації в сенсорних мережах. Описано основні їх властивості, переваги та недоліки.**

**In this article were described the classification routing protocols in Wireless Sensor Network. The basic properties, advantages and lacks are described.**

## Вступ

Безпровідні сенсорні мережі (Wireless Sensor Network*)* – це нові технології в галузі телекомунікацій та комп’ютерних мереж. Ключовим елементом WSN є сенсори, які реєструють зміни певних параметрів, наприклад, температури, тиску, вологості повітря, звуку, магнітних полів, радіації і т.п. WSN повинна задовольняти такі критерії:

• покривати задану територію і виконувати покладені на неї завдання з високою надійністю;

• сенсори, які входять до її складу, повинні самоорганізовуватися в бездротову мережу, через яку передається інформація з необхідною швидкістю без втрат;

• споживати мінімально можливу кількість енергії і при цьому працювати якнайдовше;

• швидко реагувати на події в зоні покриття;

• мати найменшу вартість.

Досягнення цих вимог значною мірою залежить від протоколів взаємодії між сенсорами та алгоритмів маршрутизації, які вони підтримують.

Метою роботи є проведення класифікації протоколів маршрутизації у WSN, їх системного аналізу та висвітлення переваг і недоліків кожного з них.

## Характеристики протоколів маршрутизації у WSN

WSN призначені для контролю навколишнього середовища. Основне завдання бездротового сенсорного вузла – сприймати й отримувати дані з певної області, обробляти їх і передавати його приймачеві, в якому розташований ужиток. Забезпечення прямого зв’язку між давачем і приймачем

може примусити вузли поширювати їхні повідомлення з такою високою потужністю, що їхні ресурси можуть бути швидко вичерпані. Тому взаємодія вузлів для забезпечення зв'язку віддалених вузлів з приймачем є обов'язковою. Отже, повідомлення поширюють проміжні вузли так, щоб маршрут з численними зв'язками або ланками до приймача був встановлений.

Під час розроблення протоколів маршрутизації для сенсорних мереж необхідно враховувати такі їх особливості:

- Вузол розгортання мережі (Node Deployment): може бути як випадковим, так і детермінованим.
- Споживання енергії (Energy Consumption): вузол може бути як джерелом, так і посередником під час передавання інформації.
- Модель представлення даних (Data Reporting Model): залежить від програми обробки.
- Неоднорідність вузлів (Node/Link Heterogeneity): вузли можуть відрізнятися за своїми властивостями.
- Відмовостійкість (Fault Tolerance): вихід з ладу окремих вузлів не повинен впливати на роботу мережі загалом.
- Масштабованість (Scalability): кількість вузлів у мережі може варіювати від декількох десятків до десятків тисяч.
- Динамічність мережі (Network Dynamics): можлива мобільність вузлів або базової станції.
- Засоби передавання (Transmission Media): Бездротові канали передавання даних.
- Зв'язність (Connectivity): наявність ізольованих вузлів або групи вузлів (залежить від щільності розподілу вузлів).
- Покриття (Coverage): кожен вузол може покривати тільки обмежену область простору.
- Агрегація даних (Data Aggregation): видалення надлишкової інформації і концентрація інформації може покращити енергетичну ефективність.
- Якість обслуговування (Quality of Service): залежить від ужитків.

WSN повинні самоорганізовуватись з ужитків, які вони використовують. Сенсори, як правило, розміщені щільно без заздалегідь визначеної топології. Зазвичай вони розкидані у межах певного регіону, з якого потрібно зібрати інформацію. Питання самоорганізації – одне з найскладніших питань у сфері розроблення технологій WSN. Ad-hoc організація мереж була першою спробою розгортання WSN.

**Flat-based протоколи**

**SPIN** (Sensor Protocols for Information via Negotiation).

Протоколи типу SPIN використовують високорівневий опис даних, щоб усунути передачу надлишкової інформації. Основна ідея таких протоколів полягає у використанні попередніх «переговорів» для уникнення повторної передачі. SPIN-протокол поширює інформацію від одного вузла до всіх інших, припускаючи, що вони є потенційною базовою станцією.

Базові ідеї протоколів SPIN:

- Обмін вимірюваними даними може бути затратний, але обміну даними про вимірювані дані (метадані) може не бути.
- Вузли повинні моніторувати і адаптуватися до змін їхніх власних енергетичних ресурсів.

Потенційно кожен вузол є базовою станцією, і інформація передається від кожного до кожного. Протокол використовує метадані і систему «переговорів». Семантика метаданих не специфікується протоколом і залежить від конкретних програм. Протокол може адаптуватися залежно від кількості енергії, що залишилась на вузлах. Протокол працює на зразок time-driven, і доставляє інформацію до всіх вузлів мережі, навіть якщо вони її не запитували.

SPIN має три стадії роботи і відповідно можуть передаватися три типи повідомлень: ADV, REQ, DATA. ADV – використовується для розповсюдження інформації про нові дані. Містить метадані. REQ – повідомлення для запиту цих даних. І, нарешті, DATA – це самі дані.

Якщо вузол хоче послати нові дані, він спочатку надсилає ADV-повідомлення своїм сусідам, далі, якщо хтось із сусідів зацікавлений в отриманні цих даних, то він надсилає REQ-повідомлення, після чого отримує дані (DATA-повідомлення).

Існує декілька протоколів сімейства SPIN:

- SPIN-1: стандартний протокол.
- SPIN-2: протокол, що використовує інформацію про залишок енергії.
- SPIN-BC: для розповсюдження broadcast повідомлень.
- SPIN-PP: для передачі повідомлень точка-точка (point-to-point).
- SPIN-EC: подібний до попереднього, але з використанням інформації про енергію (energy heuristic).
- SPIN-RL: розроблений для нестабільних каналів (lossy channels).

Протоколи сімейства SPIN добре підходять для систем, де вузли мобільні, оскільки їм потрібна тільки локальна інформація про сусідів.

Недоліком SPIN-протоколів є те, що вони не гарантують доставку даних.

**Directed Diffusion** (Алгоритм направленого поширення).

Основні елементи Directed Diffusion:

- Naming – дані позначаються за допомогою атрибутів.

Content based naming – задачі позначаються списком атрибутів – парами значень. Опис задачі визначає запит (interest) на дані, які збігаються з атрибутами.

Відстеження тварин:

| *Запит* | *Відповідь* |
|---|---|
| Опис запиту | Дані вузла |
| Type = four-legged animal | Type = four-legged animal |
| Interval = 20 ms | Instance = elephant |
| Duration = 1 minute | Location = [125, 220] |
| Location = [-100, -100; 200, 400] | Confidence = 0.85 |
| | Time = 02:10:35 |

- Interests – вузол запитує дані, посилаючи запит (interest) на визначені дані.

Безпровідна мережа періодично посилає (broadcast) запит (interest) на дані всім своїм сусідам.

Кожен вузол зберігає interest cache.

- Кожен запис відповідає індивідуальному запиту.
- Не містить інформації про WSN.
- Об'єднання (aggregation) запитів, які збігаються.

Кожен запис в кеші має кілька полів.

- Позначка про час прийому останнього запиту, що збігається.
- Кілька градієнтів: швидкість даних, тривалість, напрямок.

- Gradients – градієнти (gradients) встановлені в межах мережі, щоб доставляти дані, які збігаються із запитом.
- Reinforcement – безпровідна мережа «встановлює» (reinforce) визначені маршрути, щоб доставляти дані з більшою швидкістю (дані про швидкомінливі події).

У зв’язку з тим, що протокол орієнтований на дані, програми в сенсорах з позначеними даними використовують пари «атрибут–значення». Вузол, який запитує дані, генерує запит, який визначається залежно від атрибутів і значень, які беруться зі схеми, визначеної програмою. Приймач зазвичай вводить запит до мережі для кожної програмної задачі. Вузли оновлюють внутрішній кеш запитів отриманими запитами-повідомленнями. Вузли також мають кеш даних, де зберігаються останні повідомлення даних. Така структура допомагає визначити швидкість передавання даних. Отримавши таке повідомлення, вузли встановлюють зв'язок у відповідь ініціаторові запиту. Цей зв’язок називається градієнтом і характеризується швидкістю передавання даних, тривалістю і часом припинення. Крім цього, вузол активізує свої сенсори для збирання призначених даних. Прийом запиту-повідомлення встановлює у вузлі кілька градієнтів (або перший крок в маршруті) до джерела. Для того, щоб визначити оптимальний градієнт, використовуються позитивні і негативні підсилення. Тут алгоритм працює з двома типами градієнтів: дослідницькі і

градієнти даних. Дослідницькі градієнти призначені для встановлення та відновлення маршруту, тоді як градієнти даних використовуються для відправлення реальних даних.

SAR (Sequential Assignment Routing) є одним з перших протоколів для безпровідних сенсорних мереж, які забезпечують поняття критеріїв маршрутизації QoS. Він грунтується на асоціації пріоритетного рівня для кожного пакета. Крім того, посилання та маршрути пов'язані з метрикою, що характеризує їх потенційне надання якісних послуг. Ця метрика грунтується на затримках і витратах енергії. Потім алгоритм створює дерева з коренями, вибраними між двома сусідами приймача. Щоб зробити це, деякі параметри, такі, як пакет пріоритетів, енергетичних ресурсів і QoS-метрик, мають бути врахованими. Протокол повинен періодично перераховувати маршрути для того, щоб бути готовим в разі відмови одного з активних вузлів.

**Rumor** (Алгоритм прослуховування).

Rumor є варіантом Directed Diffusion. Він використовується, коли кількість подій (events) мала, а кількість запитів (queries) велика. За допомогою флудінга поширюються не запити, а інформація про події. Long-lived пакети, що називаються агентами, поширюють (flood) інформацію про події мережею. Коли вузол виявляє подію, він додає його до таблиці подій і генерує агента. Агенти подорожують мережею, поширюючи інформацію про локальну подію. Коли вузол генерує запит, вузол, який знає маршрут до відповідної події, може відповісти, заглядаючи в свою таблицю подій.

Переваги: немає необхідності використовувати флудінг для розповсюдження запитів; тільки один шлях між джерелом і приймачем.

Недоліки: Rumor Routing працює добре тільки тоді, коли кількість подій мала; витрати на підтримку великої кількості агентів і таблиці подій.

У цьому алгоритмі запити, згенеровані джерелом, розповсюджуються між вузлами, які контролювали подію, пов'язану із запитами. Для цього вузол, який контролює подію, вводить long-lived пакет, який називається агентом. Агенти поширюються в мережі так, що віддалені вузли «знають» про те, які вузли сприймали визначені події. Для оптимізації поведінки агентів, коли агент досягне вузол, який виявив іншу подію, агент, як і раніше, рухається далі, але додавши нову виявлену подію. Крім того, агенти містять список останніх відвіданих вузлів, так що петель можливо частково уникнути. На прийом агентів вузли можуть отримувати оновлену інформацію про події в мережі. Ці знання відображені у кешах подій вузла. При використанні кешу події вузол може легко відправити запит-повідомлення. Тим не менш, деякі вузли не можуть знати про ініціатора подій. За таких обставин, запит послідовно поширюється на один із сусідніх вузлів, обраний випадково. Після того, як запит надходить на вузол з входом, що залежить від запитуваної події в його кеші подій, запит відсилається через вивчений шлях. Після цієї процедури вартість заповнення мережі запитом є, без сумніву, меншою.

### Hierarchical-based протоколи

**LEACH** (Low-Energy Adaptive Clustering Hierarchy).

Цей протокол працює так. Вузли самоорганізовуються у кластери і вибирають cluster head. Усі вузли, які не є cluster head’ами, передають інформацію cluster head’у. Cluster head приймає дані, проводить їх обробку і передає на базову станцію. Періодично відбувається випадкова зміна cluster head’а і перекластерізація.

LEACH складається з двох фаз: організація кластерів; передача даних cluster head’у і на базову станцію.

Вибір cluster head’а поділяється на декілька етапів. На початковому етапі кожен вузол пропонує себе як cluster-head з певною ймовірністю. Вузли, які не стали cluster-head’ами, можуть стати ними згодом. Рішення приймається на основі заданої щільності cluster-head’ів в мережі. Для розподілу енергетичного навантаження мережею cluster-head'и періодично переобираються. Щойно створений вузол cluster-head розсилає свій статус іншим вузлам мережі. Кожен вузол вибирає, до якого кластера він хоче приєднатися на основі енергетичної ефективності. Коли всі вузли організувалися в кластери, cluster-head створює розклад для кожного вузла.

У фазі самоорганізації формуються кластери. Кожен cluster head посилає ADV-повідомлення за допомогою CSMA/CA протоколу. Це повідомлення містить ID вузла і заголовок, який показує, що це ADV-повідомлення. На основі сили сигналу від кожного cluster-head'а кожен вузол вибирає, до якого кластера приєднатися. Кожен вузол посилає (за допомогою CSMA/CA) join-reques- повідомлення своєму cluster-head'у. Повідомлення містить ID cluster-head'а і самого вузла. Кожен cluster-head створює TDMA розклад. Це допомагає уникнути колізій при передачі повідомлень та економію енергії.

Після цього настає фаза передачі, яка теж має декілька етапів. Вузли передають дані в свій відведений час. Після отримання повідомлень від усіх вузлів cluster-head формує свої повідомлення. Потім cluster-head передає ці повідомлення на базову станцію. Для зменшення колізій cluster-head'и використовують CDMA коди. Перед початком передачі вузол-cluster-head прослуховує канал. Якщо канал вільний, він передає інформацію на базову станцію.

Переваги протоколу LEACH:

- Використання адаптивного самоорганізовувального протоколу дає змогу розподілити енергетичне навантаження по всій мережі.
- Можна проводити обробку даних на cluster-head'і, що може зменшити кількість даних, що передаються мережею.
- Оптимальну кількість кластерів можна визначити заздалегідь залежно від топології мережі та відношення затрат на обробку/передачу інформації.
- Перша «смерть» вузла відбувається у вісім разів пізніше, ніж при використанні прямої передачі і статичних кластерних протоколів.

**PEGASIS** (Power-Efficient GAthering in Sensor Information Systems).

PEGASIS – це покращений варіант LEACH. За цим алгоритмом формуються не кластери, а ланцюжки, якими передаються дані, і один вузол їх посилає. Перевершує LEACH за енергетичними показниками.

Недоліком є великі затримки для вузлів на кінцях ланцюжка.

**TEEN** and **APTEEN** ((Adaptive) Threshold-sensitive Energy Efficient Protocol).

Цей протокол добре підходить для ужитків, критичних до часу. Він дає менші енергетичні витрати, ніж проактивні протоколи. «М'яка» межа може адаптуватися. «Жорстка» межа може варіюватися залежно від додатків.

TEEN не підходить для періодичного моніторингу, тому розроблено APTEEN – розширення TEEN як для підтримки та періодичного моніторингу, так і для реакції на критичні події. На відміну від TEEN вузол повинен зібрати і передати дані, якщо вони не були відіслані за певний період часу (count time), який встановлюється CH. Порівняно з алгоритмом LEACH, TEEN & APTEEN споживають меншу кількість енергії.

Недоліками є: накладні витрати і складність формування багаторівневих кластерів та організації порогових функцій.

**SOP** (Self-Organization Protocol).

Така архітектура підтримує різнотипні вузли. Як основу мережі використовують стаціонарні вузли роутери. Мобільні або стаціонарні сенсорні вузли надсилають інформацію на роутери. Сенсорний вузол може бути частиною мережі тільки у випадку, якщо він може передати інформацію на роутер напряму. Ця архітектура вимагає можливості адресації кожного вузла.

Переваги:

- Підходить для ужитків, де потрібний зв'язок з визначеним вузлом.
- Невеликі витрати на підтримку таблиці маршрутизації.
- Збереження збалансованої маршрутної ієрархії.
- Збереження енергії: використання обмеженої підмножини вузлів.

Недоліки:

- Цей протокол не є протоколом «на вимогу», особливо що стосується організаційної фази.
- Існування великої кількості розривів підвищує ймовірність реорганізації мережі (витратна операція).

**Location-based протоколи**

**GAF** (Geographic Adaptive Fidelity)

Цей location-based протокол враховує енергетичні ресурси вузла. Кожен вузол знає свої координати через GPS і асоціює себе з точкою на віртуальній решітці. Вузли, які вважають, що знаходяться в одній точці, рівнозначні в термінах «вартості» маршрутизації пакета. Протокол розроблено переважно для MANET, але може бути використаний і для сенсорних мереж. Алгоритм протоколу складається з трьох станів:

- Виявлення (Discovery) визначає сусідів у решітці.
- Активний.
- Сплячий.

При врахуванні мобільності, кожен вузол оцінює час свого «залишення» решітки і насилає цей час сусідам. Сусідні вузли регулюють час для сну, щоб забезпечити маршрутизацію.

Недоліки:

- Протокол погано масштабується.
- Тільки активні вузли надсилають інформацію, тому точність інформації не дуже висока.

**GEAR** (Geographic and Energy Aware Routing).

Даний алгоритм обмежує кількість запитів, які пересилаються, в directed diffusion. Він розглядає тільки певний район мережі, замість всієї мережі загалом. Кожен вузол зберігає передбачувану і навчальну вартості на досягнення WSN через своїх сусідів.

Estimated cost = f (енергія, що залишилась, відстань до точки призначення).

Навчальна вартість поширюється на одну ланку назад кожен раз, коли пакет досягне приймача. Маршрут налаштування для наступного пакета може бути скоригований.

Протокол працює двофазно.

Фаза 1: Пересилання пакетів у визначений район. Пересилається пакет сусідньому вузлу з мінімальною функцією f (найближчий до WSN і має найбільшу енергію). Якщо всі вузли знаходяться далі, ніж сам вузол-відправник, то вибирається один із сусідів на основі learned cost.

Фаза 2: Пересилання пакета в межах потрібної області.

Застосовується будь-яке рекурсивне відправлення повідомлень. Район ділиться на 4 підобласті і надсилається 4 копії пакета. Повторюється доти, поки не залишаться райони з одним вузлом.

Застосовується обмежений флудінг (коли щільність вузлів мала).

**Висновки**

Маршрутизація в безпровідних сенсорних мережах – це новий напрямок, який активно розвивається.

У межах статті розглянуто основні протоколи маршрутизації в сенсорних мережах, їх класифікацію і вимоги, які до них ставляться.

На жаль, технології енергоживлення та зберігання даних розвиваються не так швидко. Крім вдосконалення джерел енергоживлення та скорочення енергоспоживання апаратури дослідження в цій галузі передбачає збирання енергії з навколишнього середовища, розроблення ефективніших алгоритмів керування енергоспоживанням і методів оптимізації використання батарей. Особливо важливі дослідження методів визначення ступеня зарядженості батарей або їх залишку енергії. У СМ, крім того, для продовження часу життя мережі можна застосовувати протоколи, що дають змогу використовувати енергію, що залишилася у вузлах, для обчислення оптимальних комунікаційних маршрутів.

*1. Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin. 2. [DataCentric] Modelling Data-Centric Routing in Wireless Sensor Networks Bhaskar Krishnamachari, Deborah Estrin, Stephen Wicker. 3. [Dissemination] Adaptive Protocols for Information Dissemination in Wireless Sensor Networks Wendi Rabiner Heinzelman, Joanna Kulik, and Hari Balakrishnan. 4. Boukerche, A.; Nakamura, E.F.; Loureiro, A.F. Algoritms for Wireless Sensor Networks. In Algorithms and Protocols for Wireless Sensor Networks; Boukerche, A., Ed.; John Wiley & Sons: Hoboken, NJ, USA, 2009. 5. Braginsky, D.; Estrin, D. Rumor Routing Algorithm for Sensor Networks. In Proceedings of the First ACM International Workshop on Wireless Sensor Networks and Applications (WSNA), Atlanta, GA, USA, September, 2002; pp. 22–31. 6. Kulik, J.; Heinzelman, W.; Balakrishnan, H. Negotiation-based Protocols for Disseminating Information in Wireless Sensor Networks. Wirel. Netw., 2002, 8, 169–185.*