

АНАЛІЗ МЕТОДІВ УПРАВЛІННЯ ТОПОЛОГІЄЮ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ

У статті проведено аналіз методів управління топологією, які використовуються в безпроводових сенсорних мережах. Визначено недоліки та переваги зазначених методів та надано рекомендації щодо синтезу нових та вдосконаленню існуючих методів.

Жук О.В., Романюк А.В., Ткаченко Д.В. Аналіз методів управління топологією в безпроводових сенсорних мережах. Проведен аналіз методів управління топологією в безпроводових сенсорних мережах. Показано, що в залежності від цілі, задачі управління топологією розділяються на задачі управління топологією для покриття або для отримання зв'язності. Предложено рекомендації по синтезу нових і удосконаленню існуючих методів.

A. Zhuk, A. Romaniuk, D. Tkachenko Analyze topology control methods wireless sensor networks. The analysis of topology management methods and protocols in wireless sensor networks has been considered. It was shown that, depending on the purpose, topology management tasks are divided into the coverage and connectivity topology management tasks. Comparative tables of different topology management methods and protocols, and also the proposals on the synthesis of new methods and development of existing methods and protocols were given.

Ключові слова: безпроводові сенсорні мережі, методи управління топологією, географічна маршрутизація.

Вступ. Безпроводові сенсорні мережі (БСМ) або *Wireless Sensor Network (WSN)* – розподілені мережі, що складаються з маленьких сенсорних вузлів, з інтегрованими функціями моніторингу навколишнього середовища, обробки і передачі даних [1].

Одним з основних завдань оперативного управління БСМ є управління її топологією. Під топологією мережі розуміють сукупність вузлів на місцевості і каналів, що сполучають їх, у взаємному розташуванні. Топологія визначає потенційні можливості сенсорної мережі зі спостереження та доставці інформації моніторингу базовим станціям [2]. На даний час існує велика кількість методів управління топологією, одні з них направлені на побудову топології для отримання покриття, інші для отримання зв'язності (рис. 1).

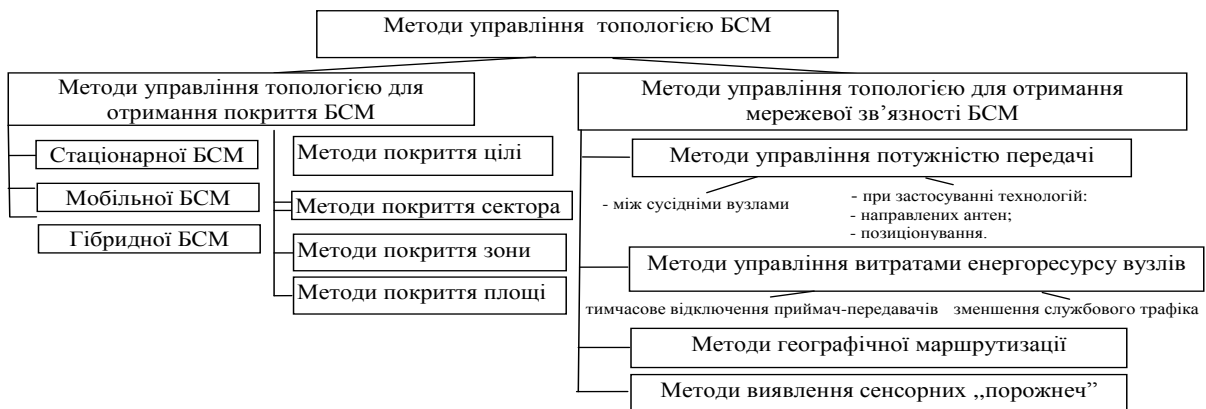


Рис. 1. Методи управління топологією в БСМ

Мета статті. Проведення аналізу існуючих методів управління топологією з метою визначення можливостей їх застосування в БСМ тактичної ланки управління військами.

Об'єкт розгляду статті. Процес управління топологією в безпроводових сенсорних мережах.

Предмет дослідження. Методи побудови топології в безпроводових сенсорних мережах.

Виклад основного матеріалу

1. Методи управління топологією для отримання покриття – забезпечують вимоги якості спостереження за цілями при використанні мінімуму енергії батарей вузлів (табл. 1).

Стаціонарні мережі

Покриття зони: метод PEAS [3] планує в часі необхідну кількість сенсорних вузлів для свого функціонування. Метод запускає два алгоритми: *Probing Environment* та *Adaptive Sleeping*. Метод *Rotating coverage* [4] – удосконалене детерміновану дискову модель покриття (вузли сусіди синхронізуються та знають радіус моніторингу).

Покриття цілі: задачею методу *Optimal Geographical Density Control* (OGDC) [5] є мінімізація частково співпадаючих радіусів моніторингу (перекриття) всіх сенсорних вузлів для випадку: $R_{\text{п}} \geq 2R_{\text{м}}$, де $R_{\text{п}}$ – діапазон передачі, $R_{\text{м}}$ – діапазон моніторингу.

Покриття площі: *Coverage Configuration* (CCP) [6] метод забезпечує гнучкість в побудові топології БСМ с різними ступенями покриття (з використанням координат вузлів). Метод *k-UC, k-NC* [7] використовує поліноміально-часовий алгоритм покриття кожної зони спостереження необхідною кількістю вузлів. Інформація про непокриті сегменти (зони) збирається центральним контролером. Недолік: централізоване управління, неможливість масштабування. Метод *Differentiated* [8] використовує розподілений алгоритм контролю щільності вузлів заснований на часовій синхронізації (рішення приймається з врахуванням необхідного ступеня покриття).

Таблиця 1

Методи управління топологією для отримання покриття

Категорія	Завдання	Рішення	Механізм реалізації	Особливості функціонування
Стаціонарні мережі	Покриття зони	PEAS [F. Ye та ін.]	Динамічне регулювання потужності	Планування вкл/викл вузлів
		<i>Rotating coverage</i> [Q. Cao та ін.]	Часова синхронізація, радіус моніторингу	Планування вкл/викл вузлів, гарантована кінцева границя затримки
	Покриття цілі, сектору	OGDC [H. Zhang та J. Hou]	Координати, фіксований дисковий радіус моніторингу	Розрахунок остаточної енергії
		<i>Sponsored Area</i>	Координати	Розрахунок сектора покриття
		<i>Extended-Sponsored Area</i>	Координати, часова синхронізація	Фіксована модель дискового покриття
	Покриття площі	CCP [X. Wang та ін.]	Координати	Реконфігуруємий рівень покриття
<i>k-UC, k-NC</i> [C. Huang та Y. Tseng]		Координати	Не одиночна дискова модель покриття	
<i>Differentiated</i> [T. Yan та ін.]		Координати, часова синхронізація	Жадібний, змінюється до рівня покриття	
Мобільні мережі	Покриття площі	VEC, VOR, <i>Minmax</i> [G. Wang та ін.]	Координати	Розрахункова геометрія, локальний, масштабований, розподілений
	Покриття площі	<i>Potential Fields</i> [A. Howard та ін.]	Діапазон, поведінка	Масштабований, розподілений, відсутня локальна передача
		DSS [N. Neo]	Координати	Масштабований, розподілений, остаточно енергія
Гібридні мережі	Покриття площі (Один мобільний сенсор)	<i>Single Robot</i> [M. Batalin, G. Sukhtame]	Координати	Розподілений, немає передачі з ретрансляціями
	Покриття площі (Множина мобільних сенсорів)	<i>Bidding Protocol</i> [G. Wang та ін.]	Координати	Переміщення для ліквідування порожнеч покриття, діаграми Вороного

Мобільні мережі

G. Wang та ін. [9] запропонували розподілений самоорганізуючий метод, який спочатку розраховує наявність непокритих зон (за допомогою діаграм Вороного) на площі спостереження, а потім вираховує позиції цілей та переміщує сенсорні вузли (VEC, VOR та *Minimax*) для зменшення непокритих зон. Методи *Potential Fields* [10] та *Distributed Self-*

Spreading (DSS) [11] використовують інформацію моніторингу для прийняття рішення з переміщення вузлів (щільність розміщення та відстань між сусідами).

Гібридні мережі

Особливу увагу необхідно приділяти розробці методів на основі застосування мобільних сенсорів – роботів, які використовуються для проведення розвідувальних операцій або відновлення мережі після бойових дій. В методі *Single Robot* [12] інформація не передається між розгорнутими вузлами (спостерігають) всі рішення приймаються мобільним роботом.

Метод *Bidding Protocol* [13] пропонує схему переміщення вузлів в гібридній мережі для ліквідування порожнеч покриття.

2. Методи (протоколи) управління топологією для отримання зв'язності

2.1. Методи управління потужністю передачі. Передбачається, що кожен вузол може змінювати потужність передачі $p_i = [p_{i_{\min}} \dots p_{i_{\max}}]$ з певним кроком дискретизації Δp . Методи управління потужністю передачі фундаментальні в досягненні мережевої енергоефективності. На даний час запропоновано ряд методів (протоколів), які використовуються для однорідних або неоднорідних сенсорних (різні типи сенсорних вузлів) мереж (однаковий або різний радіус передачі).

Однорідні мережі (однакові вузли, однаковий радіус передачі). S. Narayanaswamy та ін. пропонують розподілений протокол COMPOW [14], який намагається одночасно задовольнити три цілі: максимізація пропускнуєї спроможності всієї мережі, збільшення функціонування батарей вузлів через енергоефективні маршрути та зменшення колізій на MAC рівні (багатокритеріальна оптимізація). P. Santi і D. Blough [15] за допомогою моделювання досліджують компроміс між критичним та мінімальним радіусом передачі для побудови найбільш зв'язного компонента мережі (наприклад, 90 відсотків вузлів).

Протокол адаптовано, як для стаціонарних так і для мобільних мереж. В мобільній версії вузли переміщуються в заданий проміжок часу для визначення радіусу для зв'язності визначеної зони (компроміс між зв'язністю та витратами енергії).

Неоднорідні мережі (різні типи вузлів, різний радіус передачі). L. Kirousis та ін. [16] вперше запропонували рішення розрахунку радіусу передачі для отримання „комунікаційного графу” з високим ступенем зв'язності при мінімальних витратах енергії (NP задача для 2 та 3D мереж) – *Rang Assignment* (RA). На удосконалення RA M. Marina і S. Das пропонують протокол *Symmetric Range Assignment* (SRA), який намагається ідентифікувати (ставити мітки) на однонаправлених каналах при маршрутизації або MAC протоколах, для побудови симетричного комунікаційного графа, показуючи більші практичні переваги ніж RA. Однак D. Blough та ін. [17] доказують, що RA витрачає менше енергії ніж SRA. Багато досліджень присвячено розробці простих та практичних протоколів для побудови та підтримання ефективної топології. V. Rodoplu і T. Meng [18] запропонували розподілений алгоритм управління потужністю, який використовує інформацію місцезнаходження для мінімізації витрат енергії для зв'язку з головним вузлом. J. Pan та інші [19] розглядають дворівневу БСМ, яка складається з сенсорів кластерів, розміщених біля стратегічних зон і базових станцій (БС) місцезнаходження яких може змінюватись.

2.2. Методи управління енергоресурсом (таблиця 2). В GAF методі [21] вузли використовують координати свого розміщення для поділу площі спостереження на фіксовані квадрати. Використовується схема сну всередині кожного квадрата (вузол координатор).

В. Chen та ін. пропонують SPAN [21], для побудови енергоефективної топології (адаптивно вибирає координаторів серед всіх вузлів для ефективної передачі пакетів по сформованому маршруту та вимикає інші вузли). С. Schurgers та ін. [22] пропонують STEM метод, який використовує схему „сон” (режим „передача” та „моніторинг”).

В режимі „передача” передаються тільки дані, в режимі „моніторинг” передавачі відключаються та дані передаються тільки за подіями. R. Zheng та ін. [23] розробили асинхронну схему включення/відключення (розраховують теоретичну границю схеми прокидання при відповідній щільності).

Енергозберігаючі методи управління топологією для отримання зв'язності

Протоколи	Механізм реалізації	Мобільність	Синхронізація	Інформація про місце розташування	Розподілений
SPAN	Управління витратами енергоресурсу	Стаціонарні	Ні	Ні	Так
<i>Asynchronous Wakeup protocol</i>	Управління витратами енергоресурсу	Стаціонарні	Ні	Ні	Ні
<i>Power saving protocol</i>	Управління витратами енергоресурсу	Мобільні	Ні	Ні	Так
GAF	Управління витратами енергоресурсу	Мобільні	Ні	Так	Так
STEM	Управління витратами енергоресурсу	Стаціонарні	Ні	Ні	Так
S-MAC	Управління витратами енергоресурсу	Стаціонарні	Так	Ні	Так

2.3. *Географічна маршрутизація* (таблиця 3). Сенсорні вузли оснащені приймачами GPS (Global Position System), які дозволяють отримувати дані про своє місце розташування у вигляді: широта, довгота, висота. Маючи в своєму розпорядженні дану інформацію, сенсорні вузли мають можливість будувати та підтримувати маршрути передачі інформації, т.ч. здійснювати географічну маршрутизацію. Для мобільних БСМ запропоновано *Greedy Perimeter Stateless Routing* (GPSR) метод [24], який починає роботу з виявлення місце розташування всіх вузлів мережі та здійснює обхід „пустот” за допомогою методу периметричної маршрутизації та правила правої руки (рис. 2).

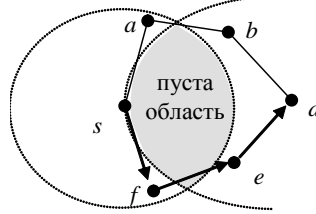


Рис. 2. Варіант обходу пустої області за допомогою GPSR

Методи *Compass Routing* та FACE-1 [25] використовують метрику мінімальної відстані між сусідами. Протокол FACE-2 [26] здійснює маршрутизацію через границі *Gabriel Graph* (GG), які побудовані в кожному вузлі. Недолік: граничні вузли витрачають більше енергії. Для удосконалення вищезазначених методів пропонується *Compass Routing* протокол, який використовує механізм зворотної роботи (повернення в жадібний режим після режиму периметричної маршрутизації). В якості удосконалення *Compass Routing* протоколу F. Kuhn і ін. [27] вводять детермінований механізм зворотної роботи (повернення в „жадібний” режим після периметричної маршрутизації та обов’язкова перевірка „периметру”).

Метод *Intermediate Node Forwarding* (INF) [28] пропонує механізм зворотного зв’язку до відправника про втрату пакета. Протокол *Active Message Relay* [29] для побудови маршруту в незв’язній мобільній мережі використовує мобільних агентів. *Geographic and Energy Aware Routing* (GEAR) [30], протокол здійснює передачу пакетів у відповідну зону мережі (висока ефективність, якщо регіон розбито на кластери, коефіцієнт ефективності швидко знижується при збільшенні площі). Недолік: використовується тільки для мереж малої розмірності.

2.4. *Виявлення сенсорних „порожнеч”* (*Sink, Black Holes, Worm holes*). Розглянуті методи географічної маршрутизації не використовують механізми виявлення та локалізації сенсорних „порожнеч”, які можуть виникати внаслідок атак на сенсорні вузли для попередження втрати пакетів.

Методи географічної маршрутизації

Протоколи	Механізм реалізації	Характеристика
GPSR [B. Karp]	Інформація про місце розташування або повний планарний граф (RNG, GG)	Правило правої руки в периметричному режимі навколо пустот
Compass Routing [E. Kranakis та ін] FACE II [P. Bose], GOAFR+	Інформація про місце розташування або повний планарний граф (GG)	Face-маршрутизація на планарних графах для запобігання маршрутних „дір”
INF [S. Douglas і ін]	Інформація про місце розташування	Передача відправнику повідомлення про відмову
Active Message Relay [Q. Li і D. Rus]	Інформація про місце розташування	Для мобільного (переміщеного) вузла досягнути незв'язного сусіда
GEAR [Y. Yu та ін]	Інформація про місце розташування, знання про коефіцієнт вартості	Знання та приблизна вартість для географічної маршрутизації та обмежена адресація в зоні

Тому розглянемо атаки та методи виявлення пошкоджених зон сенсорної мережі в наслідок дій даних атак.

Пасивні атаки. Даний тип атак не порушує нормальну роботу мережі. Вузол „зловмисник” відслідковує дані, які передаються в мережі не змінюючи їх. В деяких випадках порушення конфіденційності досягається підміною отриманих даних.

Активні атаки. В даному типі атак вузол „зловмисник” намагається модифікувати або знищити дані, що передаються, порушуючи нормальну роботу мережі. Активні атаки поділяються на два класи: внутрішні та зовнішні.

Sink / Black Holes attack – вузол „зловмисник” використовує протокол маршрутизації, для трансляції себе в якості найкоротшого маршруту, запити про маршрути вузол відслідковує в потоковому протоколі. Завданням атаки є знищення або „зациклення” пакетів, що передаються та швидке використання енергії батарей вузлів;

Wormhole attack [36] – при даному типі атаки до мережі підключаються декілька вузлів „порушників”, вузли характеризують себе, як вузли з великим ресурсом (доставка даних від вузла до базової станції), але захоплюють пакети в даній мережі та передають в іншу „зловмисну” мережу через ідентичні вузли „порушники”.

Byzantine Attack – при даному типі атаки скомпрометований вузол або набір скомпрометованих вузлів спільно здійснюють наступні атаки: „зациклення” маршрутів, відправка пакетів по неточних маршрутах, вибіркоче знищення пакетів для погіршення механізму маршрутизації.

Resource Consumption attack – ціль атаки використання обмежених мережевих ресурсів сенсорної мережі: пропускна спроможність, енергія батареї, продуктивність процесора.

Denial of Service – вузол „зловмисник” обмежує (відмова в обслуговуванні) авторизованих користувачів сервісів в мережі.

Q. Fang і ін. [31] пропонують теоретичну роботу виявлення сенсорних „порожнеч”, в якій знаходяться проблемні вузли і пропонується механізм їх обходу. M. Li і Y. Liu [32] пропонують протокол SASA для підтримання топології, який швидко виявляє структурні зміни (вражені вузли) в мережі та формує механізм взаємодії (*граничні від вузла „порушника” вузли* описують сенсорні „порожнечі” та передають інформацію про них шлюзу). A. Wood і ін. [33] пропонують JAM метод для виявлення та опису пошкодженої зони в сенсорній мережі. Метод використовує евристику (*частота помилок*) для визначення ушкодженої зони та використовує механізм її обходу (для кожного вузла використовується ID-код та інформація місцезнаходження). C. Karlof і D. Wagner [34] аналізують стійкість різних протоколів маршрутизації та алгоритмів підтримання енергоефективної топології до *Sink / Black Holes* атак. Вони показують що, популярні протоколи, такі як *Directed diffusion*, *Rumor routing* та багатомаршрутний варіант *Directed diffusion* та ін., вразливі до *Sink holes* атак. Для даних алгоритмів, які використовують жадібну передачу інформації, набагато

складніше виявити вузол „порушник” (характеризує себе, як найбільш якісний в виборі наступного кроку). A. Wood і ін. [35] розглядають варіанти захисту від „Sink holes” атак: рішення авторизації (тільки авторизовані вузли можуть змінювати маршрутну інформацію один з одним). Недолік: протокол не масштабований, криптографічні методи з відкритим ключем не можливо застосувати для БСМ в зв'язку з обмеженим ресурсами сенсорних вузлів.

ВИСНОВОК

Проведений аналіз показав, що існуючі методи управління топологією не пристосовані до умов та цілей функціонування різних типів сенсорних мереж тактичної ланки управління військами. БСМ ТЛУ відрізняються від традиційних комерційних мереж багатокритеріальністю задач управління, необхідністю резервування (неперервне функціонування із за службової необхідності), цілей (цільових функцій) управління тощо.

У ході подальших досліджень буде розроблено метод управління топологією БСМ з врахуванням вимог, які пред'являються до мереж тактичної ланки управління військами за критеріями: наявність зв'язності, задоволення вимог покриття та режимів моніторингу, мінімум витрат енергії батарей.

ЛІТЕРАТУРА

1. Міночкін А.І. Перспективи розвитку тактичних сенсорних мереж / Міночкін А.І., Романюк В.А., Жук О.В. // Збірник наукових праць. – К.: ВІТІ НТУУ „КПІ”, 2007. – № 4. – С. 16 – 22.
2. Романюк В. А. Система управління тактичними сенсорними мережами / Романюк В. А., Жук О. В., Сова О. Я. // Збірник наукових праць. – К.: ВІТІ НТУУ „КПІ”, 2008. – № 2. – С. 88 – 97.
3. F. Ye. PEAS: A Robust Energy Conserving Protocol for Long-lived Sensor Networks / F. Ye, G. Zhong, S. Lu, L. Zhang // In proceedings of International Conference on Distributed Computing Systems (ICDCS). – 2003
4. Q. Cao. Towards Optimal Sleep Scheduling in Sensor Networks for Rare-Event Detection / Q. Cao, T. Abdelzaher, T. He, J. Stankovic // In proceedings of IPSN. – 2005.
5. H. Zhang. Maintaining Sensing Coverage and Connectivity in Large Sensor Networks / H. Zhang, J. Hou // Department of Computer Science, UIUC UIUCDCS-R-2003-2351. – 2003.
6. X. Wang. Integrated Coverage and Connectivity Configuration in Wireless Sensor Networks," / X. Wang, G. Xing, Y. Zhang, C. Lu, R. Pless // In proceedings of ACM SenSys. – 2003.
7. C. F. Huang. The Coverage Problem in a Wireless Sensor Network / C. F. Huang, Y. C. Tseng // In proceedings of ACM WSNA. – 2003.
8. T. Yan. Differentiated Surveillance for Sensor Networks / T. Yan, T. He, J. Stankovic // In proceedings of ACM SenSys. – 2003.
9. G. Wang. Movement-Assisted Sensor Deployment / G. Wang, G. Cao, T. L. Porta // In proceedings of IEEE INFOCOM. – 2004.
10. A. Howard. Mobile Sensor Network Deployment using Potential Fields: A Distributed, Scalable Solution to the Area Coverage Problem / A. Howard, M. J. Mataric and G. S. Sukhatme // – 2002.
11. N. Heo. An Intelligent Deployment and Clustering Algorithm for a Distributed Mobile Sensor Network / N. Heo., P. K. Varshney // In proceedings of IEEE International Conference on Systems, Man and Cybernetics. – 2003.
12. M. A. Batalin. Coverage, Exploration and Deployment by a Mobile Robot and Communication Network / M. A. Batalin, G. S. Sukhtame // Telecommunication Systems Journal, Special Issue on Wireless Sensor Networks. – 2004. vol. 26 (2). – P. 181 – 196.
13. G. Wang. A Bidding Protocol for Deploying Mobile Sensors / G. Wang, G. Cao, T. L. Porta // In proceedings of IEEE International Conference on Network Protocol (ICNP). – 2003.

14. S. Narayanaswamy. Power control in ad hoc networks: Theory, architecture, algorithm and implementation of the COMPOW protocol / S. Narayanaswamy, V. Kawadia, R. Sreenivas, P. Kumar // In proceedings of European Wireless. – 2002.
15. P. Santi. The Critical Transmitting Range for Connectivity in Sparse Wireless Ad Hoc Networks, / P. Santi, D. Blough // In proceedings of IEEE Trans. on Mobile Computing. – 2003.
16. L. Kirousis. Power Consumption in Packet Radio Networks / L. Kirousis, E. Kranakis, D. Krizanc, A. Pelc // Theoret. Comput. Sci. – 2000. – P. 289 – 305.
17. D. Blough. On the Symmetric Range Assignment Problem in Wireless Ad Hoc Networks / D. Blough, M. Leoncini, G. Resta, P. Santi // In proceedings of the IFIP Conference on Theoretical Computer Science. – 2002.
18. V. Rodoplu. Minimum Energy Mobile Wireless Networks / V. Rodoplu, T. Meng // IEEE J. Select. Areas Comm. – 1999. – P. 1333 – 1344.
19. J. Pan. Topology Control for Wireless Sensor Networks / J. Pan, Y. T. Hou, L. Cai, Y. Shi, S. X. Shen // In proceedings of ACM Mobicom' 03. – 2003.
20. Y. Xu. Geography-informed Energy Conservation for Ad Hoc Routing / Y. Xu, J. Heidemann, D. Estrin // In proceedings of ACM Mobicom. – 2001.
21. B. Chen. Span: An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks / B. Chen, K. Jamieson, H. Balakrishnan, R. Morris // In proceedings of Mobicom. – 2001.
22. C. Schurgers. Topology Management for Sensor Networks: Exploiting Latency and Density / C. Schurgers, V. Tsiatsis, S. Ganeriwal, M. Srivastava // In proceedings of ACM Mobihoc. – 2002.
23. R. Zheng. Asynchronous Wakeup for Ad Hoc Networks / R. Zheng, J. C. Hou, L. Sha // In proceedings of ACM Mobicom. – 2003.
24. B. Karp. Greedy Perimeter Stateless Routing for Wireless Networks / B. Karp and H. T. Kung // In proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (Mobicom). – 2000.
25. E. Kranakis. Compass Routing on Geometric Networks / E. Kranakis, H. Singh, J. Urrutia // In proceedings of the 11th Canadian Conference on Computational Geometry. – 1999.
26. P. Bose. Routing with Guaranteed Delivery in Ad Hoc Wireless Networks / P. Bose, P. Morin, I. Stojmenovic, J. Urrutia // Wireless Networks. – 2001. – vol. 7. – P. 5 – 7.
27. F. Kuhn. Geometric Ad-Hoc Routing: Of Theory and Practice / F. Kuhn, R. Wattenhofer, Y. Zhong, A. Zollinger // In proceedings of ACM PODC. – 2003.
28. S. Douglas. Location proxies and intermediate node forwarding for practical geographic forwarding / S. Douglas, D. Couto, R. Morris // MIT Laboratory for Computer Science MIT-LCS-TR-824. – 2001.
29. Q. Li. Sending Messages to Mobile Users in Disconnected Ad-Hoc Wireless Networks / Q. Li, D. Rus, // In proceedings of ACM Mobicom. – 2000.
30. Y. Yu. Geographical and Energy Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks / Y. Yu, R. Govindan, D. Estrin // UCLA Computer Science Department UCLA/CSD-TR-01-0023. – 2001.
31. Q. Fang. Locating and Bypassing Routing Holes in Sensor Networks / Q. Fang, J. Gao and L. J. Guibas // In proceedings of IEEE INFOCOM. – 2004.
32. M. Li. Wireless Sensor Network for Underground Monitoring / M. Li, Y. Liu // Submitted to ACM Sensys'06. – 2004.
33. A. D. Wood, J. A. Stankovic and S. H. Son. JAM: A Jammed-Area Mapping Service for Sensor Networks / A. D. Wood, J. A. Stankovic, S. H. Son // In proceedings of 24th IEEE Real Time System Symposium (RTSS). – 2003.
34. C. Karlof. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures / C. Karlof, D. Wagner // In proceedings of 1st IEEE International Workshop SNPA. – 2003.
35. A. D. Wood. Denial of service in sensor networks / A. D. Wood, J. A. Stankovic // IEEE Computer Magazine. – 2002. vol. 35. – P. 48 – 56.