

ПРОБЛЕМИ ТА НАПРЯМКИ ДОСЛІДЖЕННЯ ПРОТОКОЛУ RPL МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ

Страшко П.В., Носков В.І.

Навчально-науковий інститут телекомунікаційних систем

НТУУ «КПІ» ім. Ігоря Сікорського, Україна

E-mail: straz0507@gmail.com; nvi2010@ukr.net

PROBLEMS AND DIRECTIONS OF THE RPL PROTOCOL RESEARCH IN THE INTERNET OF THINGS NETWORKS

In IoT networks, the RPL (Routing Protocol for Low-Power and Lossy Networks) protocol is used as a routing protocol specially designed for networks with power constraints and high channel error rates. Despite its widespread use, RPL has certain problems such as the lack of effective load balancing mechanisms, limited mobility support, and vulnerability to attacks such as black hole attacks or selective packet drop. In this regard, research into RPL is necessary to develop advanced routing algorithms that will improve the performance and reliability of IoT networks.

В мережах Інтернету речей у якості протоколу маршрутизації використовується протокол RPL (Routing Protocol for Low-Power and Lossy Networks), спеціально розроблений для мереж з обмеженнями в енергоспоживанні та високим рівнем помилок в каналах. Незважаючи на широке використання, RPL має певні проблеми такі як відсутність ефективних механізмів балансування навантаження, обмежена підтримка мобільності, вразливості до атак, таких як атака «чорна діра» або селективне відкидання пакетів. У зв'язку з цим дослідження RPL є необхідним для розробки вдосконалених алгоритмів маршрутизації, які сприятимуть покращенню продуктивності та надійності IoT-мереж.

Інтернет речей (IoT) забезпечує інтеграцію численних сенсорних пристроїв у різних галузях, зокрема в промисловості, медицині, транспорті та розумних містах. Одним із головних викликів таких мереж є забезпечення ефективної маршрутизації даних при обмежених енергетичних та обчислювальних ресурсах. Дистанційно-векторний протокол маршрутизації RPL є стандартизованим (RFC 6550) і розроблений спеціально для енергоефективних бездротових мереж із високим рівнем втрат. Його ключовою особливістю є побудова спрямованого ациклічного графа (DODAG) (рис.1), що дозволяє ефективно організовувати маршрути передачі даних та мінімізувати енергоспоживання.

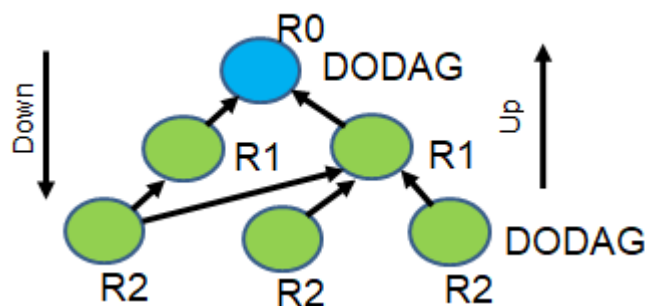


Рисунок 1. Структура DODAG (спрямований ациклічний граф).

Незважаючи на широке використання, RPL має певні обмеження. Відсутність ефективних механізмів балансування навантаження призводить до перевантаження окремих вузлів, що знижує продуктивність мережі. Обмежена підтримка мобільності ускладнює роботу в динамічних середовищах, де структура мережі постійно змінюється. Крім того, вразливості до атак, таких як атака «чорна діра» або селективне відкидання пакетів, створюють загрози для безпеки переданих даних. У зв'язку з цим дослідження RPL є необхідними для розробки вдосконалених алгоритмів маршрутизації, які сприятимуть покращенню продуктивності та надійності IoT-мереж. Оптимізація RPL можлива шляхом покращення механізмів балансування навантаження, підвищення адаптивності до мобільних пристроїв, зменшення затримок у передачі даних та впровадження вдосконалених заходів безпеки. Важливим напрямком дослідження є розробка нових алгоритмів вибору оптимальних маршрутів, що враховують як енергоспоживання, так і пропускну здатність вузлів мережі. Аналіз існуючих підходів (табл. 1) показує, що RPL поступається деяким альтернативним протоколам у певних аспектах. Зокрема, AODV (Ad hoc On-Demand Distance Vector Routing) забезпечує кращу підтримку мобільності за рахунок швидкої адаптації до змін топології, тоді як OLSR (Optimized Link State Routing Protocol) демонструє високу пропускну здатність, хоча і за рахунок збільшеного службового трафіку.

Таблиця 1. Порівняння протоколів маршрутизації.

Параметр	RPL	AODV	OLSR
Енергоспоживання (мВт)	15	35	50
Затримка передачі (мс)	50 – 100	80 – 120	30 – 70
Пропускна здатність (кбіт/с)	40 – 60	40 – 80	100 – 200
Час конвергенції (с)	0,5 – 2	0,1 – 1	2 – 5
Частота оновлення (Гц)	0,2 – 1	1 – 5	2 – 10
Втрата пакетів під час мобільності (%)	10 – 20	5 – 15	20 – 40

Параметр	RPL	AODV	OLSR
Handover Delay (мс)	100 – 300	50 – 200	200 – 500
Безпека (шифрування)	AES-128	Обмежена	Обмежена
Обсяг коду (КБ)	40 – 100	50 – 120	80 – 150
Використання CPU (%)	5 – 15	10 – 25	15 – 35
Обсяг RAM (КБ)	20 – 50	30 – 70	40 – 100
Службовий трафік (пакетів/сек)	0,2 – 1	1 – 5	2 – 10
Складність конфігурації (1-5)	3	4	5

Основними перевагами RPL є низьке енергоспоживання, ефективне управління маршрутами та мінімізація службового трафіку, що дозволяє масштабувати мережу до тисяч вузлів. Проте, він має обмежену підтримку мобільності, що може стати критичним фактором у високомобільних мережах, де AODV або інші протоколи можуть працювати ефективніше. Також зі збільшенням трафіку можливе перенавантаження вузлів. Певні проблеми з безпекою вимагають пошук ефективних методів її підвищення. Все це і визначає напрямки подальших досліджень з метою вдосконалення протоколу RPL.

Література

1. RFC 6550 - "Routing Protocol for Low-Power and Lossy Networks". [Інтернет-стандарт]. Доступ: <https://tools.ietf.org/html/rfc6550>.
2. Kharrufa, H., Al-Dubai, A., Ekonomou, E., & Wadhaj, I. (2019). RPL-Based Routing Protocols in IoT Applications: A Review. IEEE Sensors Journal, 19(15), 5982-5998. DOI: 10.1109/JSEN.2019.2916014.
3. Taghizadeh, S., Rahmani, A. M., & Othman, M. (2018). CLRPL: Context-Aware and Load Balancing RPL for IoT Networks Under Heavy and Highly Dynamic Load. IEEE Access, 6, 23277-23291. DOI: 10.1109/ACCESS.2018.2827360.
4. Матвієнко С. (2023). 6LoWPAN протокол – аналіз та впровадження у IoT. Журнал сучасних телекомунікацій, 28(2), 45-56.
5. Enhancing IoT Routing Security and Efficiency: Towards AI-Enabled RPL Protocol (2022). Journal of Internet of Things Research, 7(3), 112-130.
6. A Comprehensive Survey on Node Metrics of RPL Protocol for IoT (2021). International Journal of Communication Networks and Distributed Systems, 14(1), 56-79.
7. Kim, J., Lee, S., Park, H., & Jung, Y. (2021). Energy-Efficient RPL Enhancements for Large-Scale IoT Deployments. Sensors Journal, 21(12), 3421-3435. DOI: 10.3390/s21103421.