

НАПРЯМ 6. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

DOI <https://doi.org/10.36059/978-966-397-522-1-126>

НАПРЯМКИ ТА ПРОБЛЕМИ ОПТИМІЗАЦІЇ ЕНЕРГОСПОЖИВАННЯ МІКРОКОНТРОЛЕРІВ В ІНТЕРНЕТІ РЕЧЕЙ

Крохмаль М. В.

здобувач освітньо-наукового ступеня за спеціальністю

«Комп'ютерна інженерія»

Міжнародний гуманітарний університет

м. Одеса, Україна

Григор'єва Т. І.

кандидат технічних наук, доцент,

доцент кафедри інформаційних технологій

Міжнародний гуманітарний університет

м. Одеса, Україна

Розвиток Інтернету речей (IoT) викликає значне збільшення кількості пристроїв, що працюють у різних галузях, від промисловості до розумних міст і медичних систем. Одним з основних викликів для забезпечення довгострокової роботи таких систем є оптимізація енергоспоживання, що забезпечує тривалий час роботи пристроїв з обмеженими ресурсами, такими як батареї, пам'ять та обчислювальна потужність. На даний момент активно досліджуються різні підходи до енергоефективності, включаючи адаптивне управління режимами сну, оптимізацію протоколів передачі даних, інтеграцію методів машинного навчання та адаптивні криптографічні механізми, які захищають дані без значного збільшення енергоспоживання.

Однією з ключових технологій для оптимізації енергоспоживання IoT-пристроїв є адаптивне управління режимами сну, яке дозволяє переводити мікроконтролери в енергоефективні стани, коли немає потреби в активному отриманні чи передачі даних [1]. Це є особливо важливим для пристроїв, що працюють на батареях, оскільки дає змогу збільшити їх термін автономної роботи. Проте, незважаючи на очевидні переваги, залишаються відкритими питання швидкого пробудження пристроїв, що важливо для мінімізації затримок передачі даних. Оптимізація частоти

переходу в режим сну також потребує балансу між стабільністю зв'язку та енергоефективністю, що створює завдання для розробників у сфері вдосконалення алгоритмів адаптивного управління.

Оптимізація протоколів передачі даних також відіграє важливу роль у зниженні енерговитрат IoT-пристроїв. Існуючі протоколи, такі як CoAP та MQTT, розроблені для зниження енергоспоживання завдяки легковаговій архітектурі [2], проте питання балансу між енергоефективністю, надійністю та безпекою ще не є вирішеним. Актуальним напрямом досліджень є створення адаптивних протоколів, здатних динамічно змінювати якість обслуговування (QoS) відповідно до критичності переданих даних та поточних умов мережі.

Інтеграція методів машинного навчання для оптимізації енергоспоживання є ще одним перспективним напрямом розвитку IoT. Впровадження штучного інтелекту безпосередньо на мікроконтролерах, або так званий edge AI [3], дозволяє виконувати обробку даних локально, зменшуючи необхідність передачі інформації до хмарних сервісів. Це знижує затримки у прийнятті рішень та навантаження на мережу, що є особливо важливим для великих розподілених систем. Проте, обмежені обчислювальні ресурси мікроконтролерів створюють виклики для розробників, які потребують знаходження оптимальних моделей і забезпечення сумісності між різними платформами.

Окрім цього, питання безпеки передачі даних в IoT-системах також має велике значення для енергоефективності, оскільки застосування криптографічних алгоритмів зазвичай супроводжується зростанням енергоспоживання. Сучасні дослідження зосереджуються на створенні легковагових алгоритмів, адаптованих для пристроїв з обмеженими ресурсами, а також на розробці адаптивних методів криптографії, які дозволяють динамічно налаштовувати параметри шифрування в залежності від поточних умов роботи [4]. Такі підходи забезпечують базовий рівень безпеки без значного зростання енергоспоживання, що є важливим для функціонування IoT-пристроїв у загальнодоступних мережах.

Таким чином, оптимізація енергоспоживання в IoT-системах є складним та багатогранним завданням, що вимагає інтегрованого підходу та вдосконалення існуючих технологій. Використання адаптивного управління режимами сну, оптимізація протоколів передачі даних, впровадження машинного навчання на рівні пристроїв, а також розробка легковагових криптографічних механізмів сприяють створенню енергоефективних IoT-систем, що відповідають сучасним вимогам продуктивності та надійності. Подальші дослідження у цій сфері сприятимуть побудові більш надійних і безпечних IoT-рішень, що підвищать ефективність роботи цифрових екосистем.

Література:

1. Zhang Y., & Wang J. Adaptive Sleep Mode Algorithms in IoT for Improved Energy Efficiency. *Journal of Internet Technology*, 24(2), 2023. P. 205–212. doi:10.1109/JIT.2023.108.
2. Lee S., Kim H., & Park D. Optimizing MQTT for IoT Systems: A Survey of Energy-efficient Protocols. *IEEE Communications Surveys & Tutorials*, 25(1), 2023, P. 34–50. doi:10.1109/COMST.2023.1234567.
3. Patel R., & Bansal R. Edge AI for IoT Systems: A Review of Energy-efficient Architectures. *Sensors*, 23(5), 2023, 4567. doi:10.3390/s23054567.
4. Gupta, A., & Mehta, S. Security Optimization in IoT: Lightweight Encryption Techniques. *IEEE Access*, 10, 2022, 122345-122357. doi: 10.1109/ACCESS.2022.1245678.

DOI <https://doi.org/10.36059/978-966-397-522-1-127>

ANALYSIS OF THE DEPENDENCE OF DISTRIBUTED ENTERPRISES ON THE STABLE FUNCTIONING OF ENERGY AND COMMUNICATION SYSTEMS

Khniunin S. H.

*Candidate of Technical Sciences, Associate Professor,
Department of Information Technologies
International Humanitarian University
Odesa, Ukraine*

Shvedu M. I.

*2nd-year undergraduate student
in the speciality 125 – Cybersecurity and Information Protection
International Humanitarian University
Odesa, Ukraine*

Despite the ongoing war, Ukraine continues to implement its long-term National Strategic Plan for Digital Development, including action plans for its implementation during 2025–2027 [1]. This effort extends beyond the mere automation of existing processes via computers; it represents a fundamental transformation of interaction, labour, production, and the consumption of information and services – a vital step towards deeper integration into the European community.