УДК 004.056:004.415:621.382:681.3.06

МЕТОД РОЗПОДІЛУ КРИПТОГРАФІЧНОГО НАВАНТАЖЕННЯ МІЖ МІКРОКОНТРОЛЕРАМИ В EDGE-АРХІТЕКТУРАХ НА ОСНОВІ ЕНЕРГЕТИЧНОЇ МОДЕЛІ

Інна Розломій[1], **Сергій Науменко**[2]

METHOD FOR DISTRIBUTING CRYPTOGRAPHIC LOAD BETWEEN MICROCONTROLLERS IN EDGE ARCHITECTURES BASED ON ENERGY MODEL

Inna Rozlomii[1], Serhii Naumenko[2]

[1]Черкаський державний технологічний університет, бул. Шевченка, 460, Черкаси, 18000, Україна
[2]Черкаський національний університет імені Богдана Хмельницького, бул. Шевченка, 81, Черкаси, 18031, Україна

Abstract*. The article proposes a method for energy-efficient distribution of cryptographic workload between microcontrollers in edge architectures, taking into account their energy profiles. The approach is based on dynamic assessment of residual energy, load, and reliability of nodes. The model supports adaptability to changes in the network and allows reducing total energy consumption by 18–40% compared to baseline strategies. The simulations confirmed the effectiveness of the method for distributed systems with limited resources.*

Edge-архітектури стали ключовим елементом сучасних розподілених обчислювальних систем, зокрема в контексті Інтернету речей (IoT), кіберфізичних систем та розумних середовищ. У таких середовищах значна частина обчислень переноситься ближче до джерела даних – на край мережі, де функціонують мікроконтролери з обмеженими енергетичними та обчислювальними ресурсами. Разом із цим зростає потреба в забезпеченні конфіденційності, цілісності й автентичності даних у середовищах, які не мають можливості застосовувати повнофункціональні криптографічні алгоритми [1].

Криптографічне навантаження в edge-середовищах часто є нерівномірно розподіленим, що призводить до швидкого розряджання окремих вузлів, порушення балансу енергоспоживання та зниження загальної надійності системи. У контексті обмеженого запасу енергії важливо оптимізувати розподіл криптографічних обчислень між мікроконтролерами, враховуючи їхню поточну енергетичну модель та здатність виконувати ті чи інші операції. Традиційні підходи до захисту інформації, зосереджені переважно на забезпеченні рівня стійкості алгоритмів, не враховують енергетичних характеристик пристроїв, що є критично важливим у реальних edge-сценаріях [2].

Актуальність дослідження полягає у необхідності розробки методів енергетично доцільного використання криптографічних механізмів у децентралізованих обчислювальних середовищах. Визначальними є поняття криптографічного навантаження, під яким розуміється сукупність обчислень, пов’язаних із шифруванням, хешуванням, генерацією ключів тощо, та енергетичної моделі мікроконтролера – узагальненого представлення залежності споживаної енергії від типу операцій, частоти використання периферійних модулів і навантаження на ядро.

Проблема полягає в тому, що відсутність адаптивного механізму розподілу криптографічного навантаження з урахуванням енергетичних характеристик призводить до нераціонального використання ресурсів, скорочення часу автономної роботи edge-вузлів і

зниження загальної безпеки системи через нерівномірне навантаження на окремі вузли мережі.

Метою статті є розробка методу розподілу криптографічного навантаження між мікроконтролерами в edge-архітектурах з урахуванням їхньої енергетичної моделі для забезпечення енергоефективної та збалансованої обробки даних у розподілених середовищах.

Для ефективного розподілу криптографічного навантаження між мікроконтролерами в edge-архітектурах важливо враховувати енергетичну доцільність виконання кожної операції. Енергоспоживання кожного вузла залежить від типу криптографічної операції, обраного алгоритму, тактової частоти, тривалості виконання задачі, режиму роботи мікроконтролера та його технічних характеристик. Схема процесу енергоефективного розподілу криптографічного навантаження між вузлами edge-мережі представлена на рис. 1.

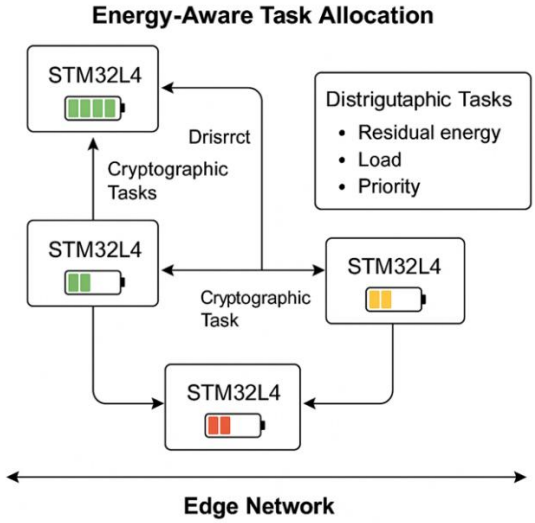

Рисунок 1 – Енергоефективний розподіл завдань між мікроконтролерами STM32L4 в периферійній мережі

Схема на рис. 1 демонструє механізм передавання задач з урахуванням залишкової енергії та поточного навантаження мікроконтролерів.

Загальне енергоспоживання мікроконтролера обчислюється як (1).

$$E = E_{idle} + \sum_{i=1}^{n} E_{op}(A_i, f, m) \quad (1)$$

де E – загальна спожита енергія за певний період часу, E_{idle} – енергія в режимі очікування або сну, $E_{op}(A_i, f, m)$ – енергія, витрачена на виконання i-тої криптографічної операції A_i за частоти f і режиму роботи m, n – кількість виконаних криптографічних операцій.

Для кількісного аналізу енергетичних витрат під час виконання криптографічних операцій на edge-пристроях було розраховано орієнтовні показники енергоспоживання (2) для трьох алгоритмів: AES-128, Ascon-128 та GIFT-COFB. Вихідними параметрами для розрахунку були середній струм споживання під час виконання операції та час її виконання на мікроконтролері STM32L4 при напрузі живлення 3.3В.

$$E_{op} = V \cdot I_{op} \cdot t_{op} \quad (2)$$

де I_{op} – середній струм споживання, t_{op} – час виконання операції.

Таблиця 1 Порівняння енергоспоживання криптоалгоритмів на мікроконтролері STM32L4

Алгоритм	Середній струм, мА	Час виконання, мс	Спожита енергія, мкДж
AES-128	8.2	1.5	40.59
Ascon-128	5.7	1.1	20.65
GIFT-COFB	4.3	0.9	12.77

Ці дані свідчать про значну різницю в енергоспоживанні між класичними та полегшеними алгоритмами. Так, використання GIFT-COFB дозволяє зменшити витрати

енергії майже втричі порівняно з AES-128, що критично важливо для автономних edge-пристроїв з обмеженим енергетичним запасом.

Задача оптимального розподілу криптографічного навантаження в edge-архітектурі формалізується як задача мінімізації сумарного енергоспоживання мережі за умови виконання заданого обсягу операцій шифрування, хешування або автентифікації у межах допустимого часу. Нехай у мережі наявні N мікроконтролерів, кожен з яких має власний енергетичний профіль, що включає залишковий заряд акумулятора, ефективність виконання криптографічних операцій, а також поточну завантаженість. Для кожного вузла визначається функція енергетичної вартості виконання криптографічної задачі. Цільова функція передбачає мінімізацію сумарного енергоспоживання при виконанні всіх задач у системі (3).

$$min \sum_{i=n}^{M} E_{i,j} \quad (3)$$

де E_i – енергія, необхідна для виконання задачі i на вузлі j, M – кількість криптографічних задач. Обмеження включають допустимий час обробки T_{max}, мінімальний рівень залишкової енергії B_{min} та пропускну здатність комунікаційного каналу, яка може обмежувати передачу зашифрованих даних. Також враховується коефіцієнт надійності вузла, що відображає його історичну стабільність, доступність та здатність працювати в критичних умовах.

Оптимізаційна модель підтримує динамічний характер edge-середовища, де кількість вузлів може змінюватися, а рівень доступної енергії – коливатися з часом. Урахування змінних параметрів у режимі реального часу дозволяє ефективно адаптувати розподіл навантаження відповідно до поточного стану системи, підтримуючи баланс між енергетичною ефективністю та виконанням криптографічних вимог.

Розподіл криптографічних задач між вузлами edge-мережі здійснюється за допомогою евристичного методу, який базується на локальній оцінці енергетичної доцільності. Для кожного вузла обчислюється коефіцієнт енерговитратності, що враховує як споживання енергії на виконання задачі, так і залишковий заряд. Завдання призначається тому вузлу, для якого цей коефіцієнт є мінімальним і який відповідає всім обмеженням за часом та ресурсами. У разі рівних показників перевага надається вузлам із меншим завантаженням або з вищим пріоритетом за надійністю.

Алгоритм допускає часткову переорієнтацію завдань у разі зміни ситуації в мережі, зокрема виходу вузла з системи, критичного зниження його енергетичних показників або зміни пріоритетів задач. Завдяки своїй гнучкості метод підтримує масштабування мережі до десятків вузлів без значного зростання часу обчислень. Крім того, врахування контекстних показників – таких як температура навколишнього середовища, частота збоїв, відстань до інших вузлів – дозволяє підвищити стійкість мережі до зовнішніх впливів і забезпечити збереження безперервності криптографічного захисту в реальному часі.

Запропонований підхід не потребує централізованого керування, а може бути реалізований у децентралізованому режимі із взаємоузгодженням між вузлами за допомогою легких протоколів комунікації. Це забезпечує незалежність від єдиної точки відмови та стійкість до атак на координаційний центр. У випадках, коли частина задач потребує більшого обсягу обчислень, можливе використання гібридного сценарію з частковим переміщенням обробки до більш потужних пристроїв (наприклад, fog-вузлів), що також враховується у процесі призначення задач.

Для оцінки ефективності запропонованого методу розподілу криптографічного навантаження було проведено моделювання edge-мережі з використанням набору з 20 мікроконтролерів, що мають різні енергетичні профілі, наближені до характеристик STM32L4. Було порівняно три стратегії: запропонований енергопрофільний метод, рівномірний розподіл задач між вузлами та випадкове призначення. Для кожного сценарію моделювався оброблюваний масив даних, що потребував криптографічної обробки у вигляді автентифікованого шифрування, та вимірювались ключові метрики.

Результати моделювання показали, що запропонований підхід зменшує сумарне енергоспоживання системи на 18–25% порівняно з рівномірним розподілом і до 40%

порівняно з випадковим. Пікове навантаження на окремі вузли знизилось у середньому на 30%, що суттєво вплинуло на загальний баланс роботи мережі. Завдяки адаптивному врахуванню залишкового заряду автономність найвразливіших вузлів зросла на 22–28%, що дозволяє відтермінувати їхнє виключення з роботи та продовжити функціонування критичних каналів зв'язку.

Ефективність трьох стратегій розподілу криптографічного навантаження продемонстровано на рис. 2, де відображено динаміку сумарного енергоспоживання залежно від кількості оброблених задач.

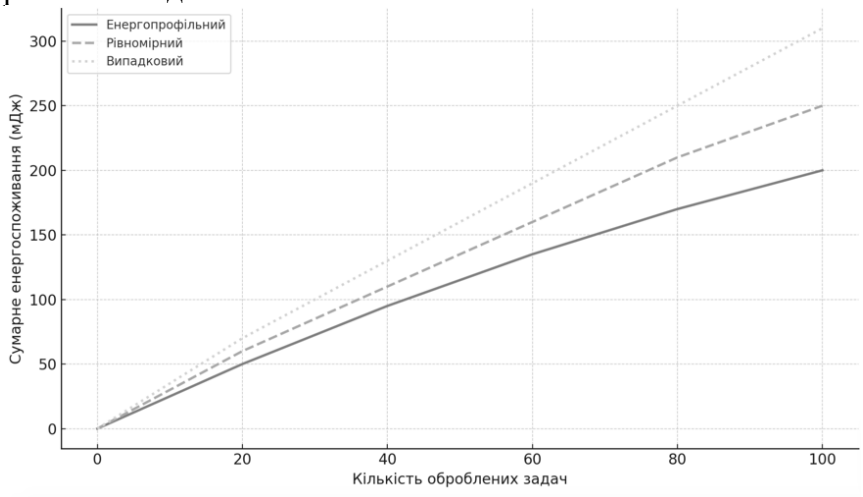

Рисунок 2 – Сумарне енергоспоживання при різних стратегіях розподілу задач

Як видно з рис. 2 енергопрофільна стратегія забезпечує найменше зростання сумарного енергоспоживання в порівнянні з рівномірним і випадковим розподілом. Це свідчить про доцільність адаптивного підходу при роботі з edge-пристроями, які мають обмежені енергетичні ресурси. Також зафіксовано зниження частоти перевантаження мережі завдяки зменшенню обсягу міжвузлової комунікації: у запропонованій моделі завдання виконуються там, де це найбільш енергетично доцільно, без надмірного пересилання даних.

Отримані результати підтверджують переваги запропонованого підходу у плані енергетичної ефективності, масштабованості та стійкості до змін стану мережі. Разом з тим, метод має певні обмеження: не враховується складна топологія або мобільність вузлів, а також потенційні атаки на механізм призначення задач, зокрема маніпуляції енергетичними показниками.

До переваг методу можна віднести низьку обчислювальну складність алгоритму розподілу, що дозволяє реалізувати його на самих edge-пристроях без звернення до центрального вузла. Також відзначається гнучкість і адаптивність до енергетичних коливань у реальному часі. Слабким місцем залишається потреба в постійному моніторингу стану вузлів, що може створювати додаткове навантаження на канал зв'язку або потребувати локального буферизованого обліку.

Подальші дослідження доцільно спрямувати на інтеграцію топологічної адаптації до змін конфігурації мережі, впровадження механізмів довіри для перевірки достовірності енергетичних параметрів вузлів та вивчення поведінки системи у випадку часткової втрати зв'язку або появи нових вузлів. Це дозволить розширити можливості методу і наблизити його до реальних умов експлуатації в критичних кіберфізичних системах.

Бібліографія

1. Rozlomii, I., Naumenko, S., Mykhailovskyi, P., & Monarkh, V. (2024, October). Resource-Saving Cryptography for Microcontrollers in Biomedical Devices. In 2024 IEEE 5th KhPI Week on Advanced Technology (KhPIWeek) (pp. 1-5). IEEE.
2. Rozlomii, I., & Naumenko, S. (2024). Моделювання взаємовпливу інформаційної безпеки та обчислювальних витрат у вбудованих пристроях. Computer-Integrated technologies: education, science, production, (57), 139-145.