МЕТОД ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ У СИСТЕМАХ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ

Євгеньєв А.М., Сидоренко З.М., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Промисловий Інтернет речей (Industrial Internet of Things, IIoT) - це технологія, що поєднує інтелектуальні датчики, пристрої та програмне забезпечення для автоматизації, моніторингу та управління промисловими процесами. Однією з ключових проблем IIoT є забезпечення цілісності даних, тобто гарантія того, що передані та збережені дані залишаються незмінними, точними та достовірними без несанкціонованих змін або пошкоджень [1].

Забезпечення цілісності даних у системах IIoT є критичним аспектом інформаційної безпеки, оскільки порушення цілісності може призвести до неправильного функціонування обладнання, аварій та втрати довіри до системи. У промисловому середовищі це питання набуває ще більшого значення, зважаючи на автоматизовані процеси та великі об'єми взаємодіючих пристроїв.

Метою доповіді є аналіз методів забезпечення цілісності даних у системах промислового Інтернету речей. Розгляд методу забезпечення цілісності на основі використання завадостійких кодів.

На даний час для забезпечення цілісності даних в IIoT використовуються різні методи [1]:

– криптографічні геш-функції на основі алгоритмів SHA-2, SHA-3 для формування контрольної суми (гешу);

– цифровий підпис на основі алгоритмів RSA, ECDSA, постквантових схем на решітках;

– протоколи безпечної передачі TLS, DTLS, MQTT-SN з шифруванням, що підтримує контроль цілісності (наприклад, HMAC);

– апаратні модулі захисту (HSM, TPM) перевірки автентичності даних на рівні пристроїв;

– запис даних від пристроїв у блокчейн або розподілений реєстр, в яких будь-яка зміна залишає цифровий слід.

Але на даний час ці методи не в повній мірі забезпечують цілісність даних. Існує багато загроз, яким традиційні системи не в повній мірі можуть протистояти. Також традиційні криптографічні методи (AES, RSA, ECC) не можуть виправляти помилки, спричинені шумами або апаратними збоями. Більшість з них не забезпечать стійкість у постквантовий період.

Саме тому перспективним рішенням є поєднання криптографії та завадостійкого кодування. Кодові криптосистеми (McEliece, Niederreiter) можуть забезпечити одночасно шифрування та перевірку на цілісність, що особливо актуально у постквантовий період [2-4].

Дані криптосистеми засновані на застосуванні одного з підкласів альтернативних кодів - кодів Гоппи, які мають найкращі характеристики в

класі лінійних блокових кодів. Характерною властивістю кодів Гоппи є той факт, що є велика кількість способів формування коду із заданими параметрами, що потенційно може вирішити задачу не тільки забезпечення високої стійкості до перешкод, але і цілісності даних в системах промислового Інтернету речей [5]. У завадостійких кодах як і в кодах автентифікації послідовності, що передаються, містять спеціальну надлишкову інформацію. Різниця полягає в тому, що якщо у звичайних завадостійких кодах є одне правило кодування, що відповідає фіксованому коду, то в кодах автентифікації є багато правил кодування, з яких передавач чи приймач може обирати для використання одне конкретне (таємне) правило. Саме тому звичайні завадостійкі коди не можуть бути використані для забезпечення цілісності даних. Одним із небагатьох класів лінійних блокових кодів, що мають безліч законів формування при фіксованих параметрах коду, є коди Гоппи, що явно стало причиною спроб створення на їх основі систем криптозахисту.

Коди Гоппи утворять великий клас, найважливішими підкласами якого є коди БЧХ, коди Срівестави, узагальнення Ченя-Чоя кодів БЧХ. Для даного класу доведене існування кодів, лежачих на границі Варшамова-Гілберта. Крім того, велике число багаточленів G(x), що визначають код з параметрами не гірше заданих, дозволяє використовувати дані коди для забезпечення цілісності даних, а можливість визначення всієї множини кодових слів за допомогою одного багаточлена дозволяє останній використовувати як ключ.

Стійкість схем, побудованих на кодах Гоппи заснована на складності рішення відомої в теорії завадостійкого кодування важко вирішуваної задачі декодування випадкового коду. Також дані системи мають достатньо високу швидкість (в порівнянні з криптосистемами RSA, ECC і ін.) перетворень. Крім того кодові криптосистеми залишаються стійкими навіть при використанні квантових обчислень [5]. Їх застосування дозволяє сумістити в один механізм процедури захисту інформації і завадостійкого кодування.

Таким чином, слід припустити, що використання для захисту від помилок кодів Гоппи дозволить додатково вирішувати такі завдання, як забезпечення цілісності та інформаційної скритності каналів передачі даних у системах IIoT.

Список літератури

1. Сирадоєв А.О., Можаєв О.О. (2024). Дослідження споживчого і промислового Інтернету речей.

2. Y. Melenti et al. Development of post-quantum cryptosystems based on the Rao-Nam scheme. (2025) Eastern-European Journal of Enterprise Technologies, 1 (9(133)), pp. 35-48.

3. Керничний В., Сєвєрінов О.В. Аналіз стійкості криптосистеми McEliece // Global Cyber Security Forum: матеріали Першого міжнародного науково-практичного форуму, 14 – 16 листопада 2019 р. – Харків: ХНУРЕ, 2019. – С. 55–56.

4. Шипілов Д.В., Халімов Г.З. Аналіз постквантової криптосистеми McEliece. // Комп'ютерні та інформаційні системи і технології, ХНУРЕ, 2019. - С. 83–84.

5. Bernstein, Daniel J., Buchmann, Johannes, and Dahmen, Erik. Post-Quantum Cryptography. – 2009, Springer-Verlag, Berlin-Heidleberg. – 245 p.