СЕКЦІЯ 3

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

УДК 004.056(477)

Ігор САПІЖУК, Богдан БАРАННІК, Павло БИЛЕНЬ

Західноукраїнський національний університет

ЗАСТОСУВАННЯ СТЕГАНОГРАФІЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ТА АВТЕНТИЧНОСТІ ДАНИХ В ІНТЕРНЕТІ РЕЧЕЙ

Вступ. В умовах стрімкого розвитку Інтернету речей (IoT) та зростаючої кількості підключених пристроїв, питання захисту конфіденційності та автентичності даних набуває особливої актуальності. Щоденно мільярди IoT-пристроїв генерують та передають величезні обсяги чутливої інформації, яка потребує надійного захисту від несанкціонованого доступу та модифікації. Традиційні методи криптографічного захисту не завжди можуть бути ефективно застосовані в умовах обмежених обчислювальних ресурсів IoT-пристроїв. У цьому контексті стеганографія, як метод приховування факту передачі інформації, може стати ефективним додатковим інструментом забезпечення безпеки даних в IoT-системах.

Мета: дослідження можливостей методів застосування стеганографічних технік для підвищення рівня захисту конфіденційності та забезпечення автентичності даних, що передаються між пристроями в мережах Інтернету речей. У рамках дослідження планується дослідити можливості комбінування криптографічних та стеганографічних методів захисту та дослідити енергоефективність при реалізації комбінованих методів захисту IoT.

1. Дослідження можливості комбінування криптографічних та стеганографічних методів захисту даних в IoT

У сучасному світі технологій Інтернет речей (IoT) став невід'ємною частиною нашого повсякденного життя. З кожним днем кількість підключених пристроїв зростає, що створює нові виклики для забезпечення безпеки даних. Особливу увагу слід приділити питанню комбінування криптографічних та стеганографічних методів захисту інформації в IoT-системах, оскільки саме такий підхід може забезпечити комплексний захист чутливих даних [1].

Основною проблемою при впровадженні традиційних методів захисту IoT-пристроїв є їхні обмежені обчислювальні можливості та ресурси. Багато IoT-пристроїв працюють від батарей, мають обмежену пам'ять та процесорну потужність, що ускладнює використання складних криптографічних алгоритмів. У цьому контексті стеганографічні методи можуть стати ефективним доповненням до легких криптографічних алгоритмів, створюючи додатковий рівень захисту без значного навантаження на системні ресурси.

Криптографічні методи забезпечують конфіденційність даних шляхом їх шифрування, роблячи інформацію нечитабельною для сторонніх осіб. Однак сам факт передачі зашифрованих даних може привернути увагу зловмисників. Саме тут на допомогу приходить стеганографія, яка дозволяє приховати сам факт

передачі секретної інформації. При цьому важливо враховувати особливості IoT-комунікацій, такі як обмежена пропускна здатність каналів зв'язку та необхідність передачі даних у реальному час і[2].

Для ефективного поєднання цих двох підходів необхідно розробити спеціалізовані алгоритми, які враховують специфіку IoT-середовища. Наприклад, можна використовувати легкі криптографічні алгоритми для шифрування найбільш критичних даних, а потім приховувати їх у звичайному мережевому трафіку за допомогою стеганографічних методів [3]. Це дозволить створити подвійний захист без значного впливу на продуктивність системи. Важливим аспектом є вибір відповідних стеганографічних контейнерів для IoT-даних.

В якості таких контейнерів можуть виступати службові поля мережевих протоколів, часові інтервали між пакетами даних, або навіть шаблони енергоспоживання пристроїв. При цьому необхідно забезпечити стійкість стеганографічного каналу до різних типів атак та спроб виявлення прихованої інформації [4].

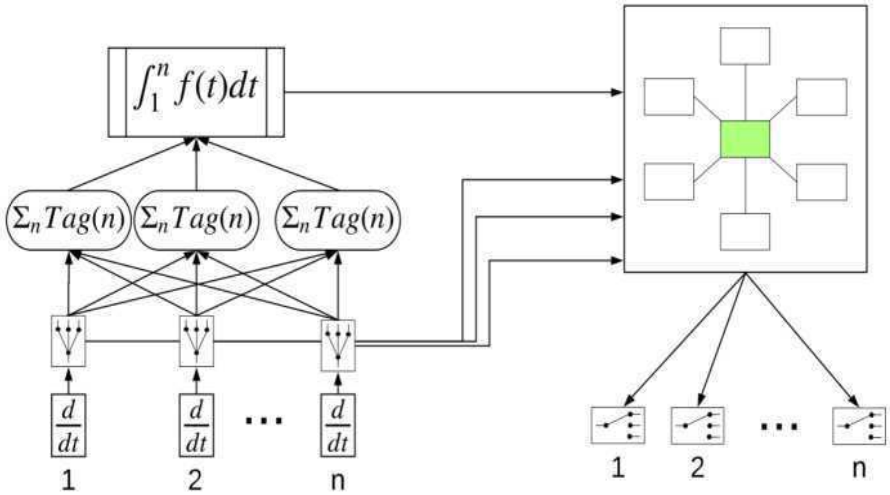

Рисунок 1 - Схема процесу обробки та агрегації даних із декількох джерел чи пристроїв

Одним з перспективних напрямків є використання адаптивних алгоритмів, які можуть динамічно змінювати параметри захисту залежно від поточних умов роботи системи.

Наприклад, при виявленні підозрілої активності система може автоматично посилювати рівень захисту, змінюючи алгоритми шифрування та методи стеганографічного приховування даних.

Особливу увагу слід приділити питанням управління ключами та синхронізації між пристроями при використанні комбінованого захисту. Необхідно розробити ефективні механізми розповсюдження та оновлення криптографічних ключів, а також забезпечити надійну синхронізацію параметрів стеганографічних алгоритмів між усіма учасниками обміну даними [5].

При розробці комбінованих методів захисту важливо враховувати можливі сценарії атак та вразливості системи. Необхідно проводити регулярний аналіз безпеки та оцінку ефективності застосованих методів захисту. Це дозволить своєчасно виявляти та усувати потенційні загрози, а також вдосконалювати існуючі механізми захисту.

Впровадження комбінованих методів захисту в IoT-системи потребує також розробки відповідних стандартів та протоколів. Це дозволить забезпечити сумісність різних пристроїв та спростити процес інтеграції нових рішень у існуючі системи. Важливо, щоб розроблені стандарти були достатньо гнучкими для адаптації до різних сценаріїв використання та типів IoT-пристроїв[6].

Для практичної реалізації комбінованого захисту необхідно також розробити відповідні інструменти та програмне забезпечення. Це можуть бути бібліотеки криптографічних та стеганографічних алгоритмів, оптимізовані для роботи на IoT-пристроях, а також засоби моніторингу та управління системою безпеки.

У подальшому розвитку цього напрямку важливо враховувати нові технологічні тренди та загрози безпеці. Наприклад, з появою квантових комп'ютерів може виникнути необхідність у розробці нових криптографічних алгоритмів, стійких до квантових обчислень. Відповідно, методи стеганографічного захисту також повинні еволюціонувати для забезпечення належного рівня безпеки [7].

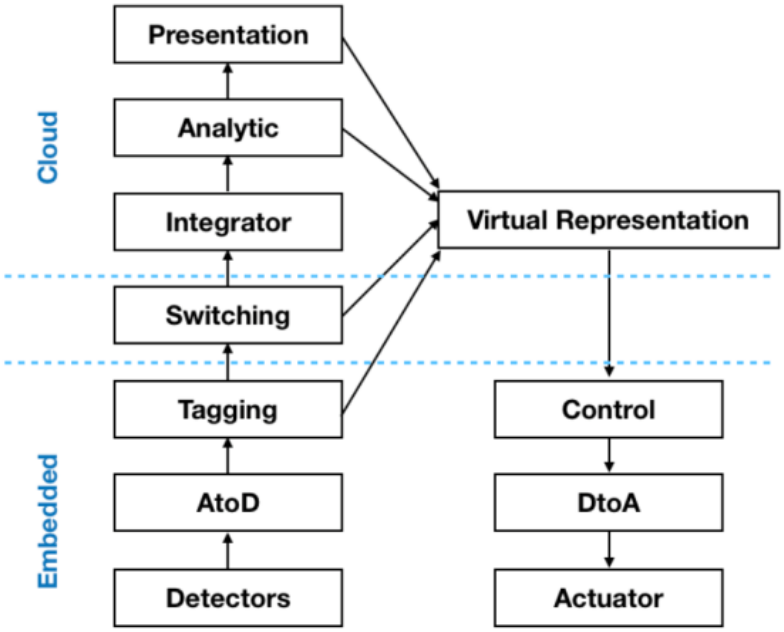

Рисунок 2 - Схема обробки даних у системі IoT

Комбінування криптографічних та стеганографічних методів захисту даних в IoT є перспективним напрямком досліджень, який потребує комплексного підходу та врахування багатьох факторів. Успішна реалізація такого підходу дозволить створити надійну систему захисту, здатну протистояти сучасним загрозам безпеці в умовах обмежених ресурсів IoT-пристроїв.

2. Енергоефективність при реалізації комбінованих методів захисту в IoT-системах

IoT стрімко інтегрується в усі сфери нашого життя, питання енергоефективності при забезпеченні безпеки даних стає все більш актуальним. Особливо гостро ця проблема постає при впровадженні комбінованих методів захисту в IoT-системах, де кожен пристрій має обмежений заряд батареї та обчислювальні ресурси.

Використання комбінованих методів захисту, які поєднують криптографічні та стеганографічні підходи, створює додаткове навантаження на IoT-пристрої. Це призводить до підвищеного споживання енергії, що може значно скоротити час автономної роботи пристроїв. Тому при розробці систем захисту необхідно знаходити оптимальний баланс між рівнем безпеки та енергоефективністю.

Одним з перспективних напрямків вирішення цієї проблеми є впровадження адаптивних алгоритмів захисту. Такі алгоритми здатні динамічно регулювати інтенсивність захисних механізмів залежно від поточного рівня заряду батареї та важливості даних, що обробляються. Наприклад, при низькому заряді батареї система може автоматично переходити на більш легкі лгоритми шифрування або зменшувати обсяг стеганографічно прихованої інформації. Важливим аспектом є також оптимізація процесів обробки даних на рівні апаратного забезпечення. Використання спеціалізованих апаратних прискорювачів для виконання криптографічних операцій може значно знизити енергоспоживання порівняно з програмною реалізацією тих самих алгоритмів. Це особливо актуально для пристроїв, які постійно обробляють великі обсяги даних.

При розробці енергоефективних методів захисту необхідно також враховувати особливості мережевої взаємодії IoT-пристроїв. Правильний вибір протоколів передачі даних та оптимізація мережевого трафіку можуть значно вплинути на загальне енергоспоживання системи. Наприклад, використання легких протоколів шифрування та компактних форматів даних дозволяє зменшити обсяг переданої інформації та, відповідно, енергетичні витрати на її передачу.

Особливу увагу слід приділити методам стеганографічного приховування даних, які потребують мінімальних енергетичних витрат. Це може бути досягнуто шляхом використання природних особливостей роботи IoT-пристроїв, таких як часові інтервали між передачею пакетів даних або шаблони енергоспоживання, як стеганографічних контейнерів.

Важливим фактором є також розробка ефективних методів управління ключами та параметрами захисту. Правильна організація процесів генерації, розповсюдження та оновлення криптографічних ключів може значно вплинути на загальну енергоефективність системи. При цьому необхідно забезпечити надійний захист самих ключів та параметрів, що використовуються для стеганографічного приховування даних.

Перспективним напрямком є також використання методів машинного навчання для оптимізації енергоспоживання систем захисту. Алгоритми штучного інтелекту можуть аналізувати патерни використання пристроїв та автоматично адаптувати параметри захисту для досягнення оптимального балансу між безпекою та енергоефективністю.

У контексті енергоефективності важливо також враховувати можливості відновлення енергії з навколишнього середовища. Використання технологій енергозбору (energy harvesting) може допомогти компенсувати додаткові енергетичні витрати, пов'язані з реалізацією механізмів захисту. Це особливо актуально для IoT-пристроїв, що працюють у віддалених або важкодоступних місцях.

Забезпечення енергоефективності при реалізації комбінованих методів захисту в IoT-системах є комплексним завданням, яке потребує врахування багатьох факторів та застосування інноваційних підходів. Успішне вирішення цієї задачі дозволить створити надійні та довговічні системи IoT, здатні забезпечити належний рівень захисту даних без надмірного споживання енергії

Висновок. У результаті проведеного дослідження було розглянуто актуальні проблеми захисту даних в системах Інтернету речей та запропоновано комплексний підхід до їх вирішення шляхом комбінування криптографічних та стеганографічних методів. Особлива увага була приділена питанню енергоефективності при реалізації цих методів захисту, враховуючи обмежені ресурси IoT-пристроїв.

Було встановлено, що використання адаптивних алгоритмів захисту та спеціалізованих апаратних рішень дозволяє значно оптимізувати енергоспоживання при забезпеченні належного рівня безпеки. Запропоновані підходи до стеганографічного приховування даних з використанням природних особливостей роботи IoT-пристроїв демонструють перспективність у контексті мінімізації додаткових енергетичних витрат.

Результати дослідження показують, що ефективне поєднання криптографічних та стеганографічних методів з урахуванням енергетичних обмежень дозволяє створити надійну систему захисту даних в IoT. Подальший розвиток цього напрямку може бути пов'язаний з впровадженням технологій машинного навчання для оптимізації параметрів захисту та дослідженням можливостей використання альтернативних джерел енергії для IoT-пристроїв.

Перелік використаних джерел.

1. Аль-Судані О.І., Ковальчук Л.В., Кучинська Н.В. Методи стеганографічного захисту даних в IoT-системах. Захист інформації. 2023. Т. 25, № 2. С. 73-82.

2. Бурячок В.Л., Толюпа С.В., Складанний П.М. Інформаційна безпека та кібербезпека IoT-пристроїв: монографія. Київ: ДУТ, 2022. 284 с.

3. Гнатюк С. О., Кінзерявий В. М., Бурячок В. Л. Теоретичні основи побудови систем захисту інформації в IoT. Безпека інформації. 2023. Т. 29, № 1. С. 15-24.

4. Корченко О.Г., Терейковський І.А., Заболотний В.В. Енергоефективні методи криптографічного захисту в системах IoT. Вісник Національного технічного університету України КПІ. Серія: Радіотехніка. Радіоапаратобудування. 2022. № 88. С. 66-75.

5. Куліш С.М., Хорошко В.О., Шелест М.Є. Комбіновані методи захисту інформації в сучасних мережах IoT. Сучасний захист інформації. 2023. № 1(49). С. 28-37.

6. Юдін О.К., Бучик С.С., Чунарьова А.В. Методологія оцінювання енергоефективності систем захисту інформації в IoT. Наукоємні технології. 2022. № 2(54). С. 115-124.

7. Bondar V., Hryshchuk R., Horoshko V. Steganographic Methods for IoT Data Protection: Mathematical Models and Implementation. Cybersecurity: Education, Science, Technology. 2023. Vol. 3, No. 15. P. 88-97.