DOI: 10.18372/2310-5461.66.20333
УДК 004.77

М. С. Савка, аспірант
Національний технічний університет України
"Київський політехнічний інститут
імені Ігоря Сікорського"
https://orcid.org/0000-0003-2049-9438
e-mail: maximsavka@gmail.com

КОМПЛЕКСНА МОДЕЛЬ ЗБОРУ ДАНИХ В МЕРЕЖАХ МОБІЛЬНОГО ІНТЕРНЕТУ РЕЧЕЙ

Вступ

Дані Інтернету речей (IoT) – це великий масив інформації, що надходить від різнорідних автономних та взаємопов'язаних пристроїв. Значну частину з них можна централізовано керувати. Можуть застосовуватися як централізовані, так і децентралізовані схеми управління. Основними проблемами, які необхідно вирішити в системах IoT, є управління даними і захист даних. Важливо забезпечити надійне керування маршрутизацією та обробкою даних.

Аналіз останніх досліджень та публікацій

Сучасні IoT-системи використовують все більшу кількість різних протоколів. DDS (Data Distribution Service) і WiFi для передачі даних між пристроями, MQTT (Message Queuing Telemetry Transport), HTTP (Hypertext Transfer Protocol), XMPP (Extensible Messaging and Presence Protocol), CoAP (Constrained Application Protocol), AMQP (Advanced Message Queuing Protocol) для взаємодії та обміну даними між серверами. В IoT активно використовуються протоколи бездротового зв'язку. Супутниковий протокол M2M («Машина до машини»), технологія Bluetooth, протоколи WiFi, ZigBee і ZWave та технологія RFID (Radio-Frequency Identification) для обміну інформацією між пристроями [1].

Постановка задачі

Проектування систем IoT передбачає вирішення завдання моделювання процесів інформаційної взаємодії. Це дає змогу визначити оптимальний режим їхньої роботи з урахуванням прогнозованого трафіку. Концепція IoT полягає в забезпеченні взаємодії об'єктів, передачі даних і підтриманні надійного з'єднання. Враховуючи новизну, ключові особливості та складність структури системи IoT, на етапі проєктування ключову роль відіграє мобільна модель комплексного збору даних в IoT-мережах.

Виклад основного матеріалу

Розроблено модель збору даних, адаптовану до умов мобільного Інтернету речей. Пристрої в моделі відповідають за збір інформації про навколишнє середовище. Рівень обробки та зберігання даних вирішує задачу передачі даних, отриманих від пристрою. Для збору, обробки й зберігання даних пропонується поєднати засоби IoT, аналізу соціальних мереж і методи інтелектуального аналізу. [2]. Запропонована інтегрована модель показана на рис. 1. Ця модель вирішує завдання IoT використовуючи розумні мобільні пристрої.

Технологія fog computing може зменшити затримку передачі, підвищити пропускну здатність і покращити загальні характеристики мережі.

Використання кластеризації дає змогу значно підвищити енергоефективність мережі, зменшило складність маршрутизації даних і скоротило затримку передачі даних. Очікується, що таке поєднання існуючих технологій покращить управління агрегацією даних, необхідне для мобільних IoT-мереж [3]. У порівнянні з наявними рішеннями, модель має забезпечити менше енергоспоживання, швидший обмін даними та вищу безпеку. Для реалізації інтегрованої моделі розглянемо її основні структурні елементи (рис. 2). Розглянуті методи та алгоритми реалізуються в рамках запропонованої моделі.

Фізичний рівень. Фізичний рівень лежить в основі запропонованої моделі. На фізичному рівні розташовані датчики і пристрої. Для передачі зібраних даних використовуються бездротові мережі (рис. 3).

Більшість з них є відкритими мережами і піддаються різним видам атак. Необхідно вжити заходів для забезпечення безпеки.

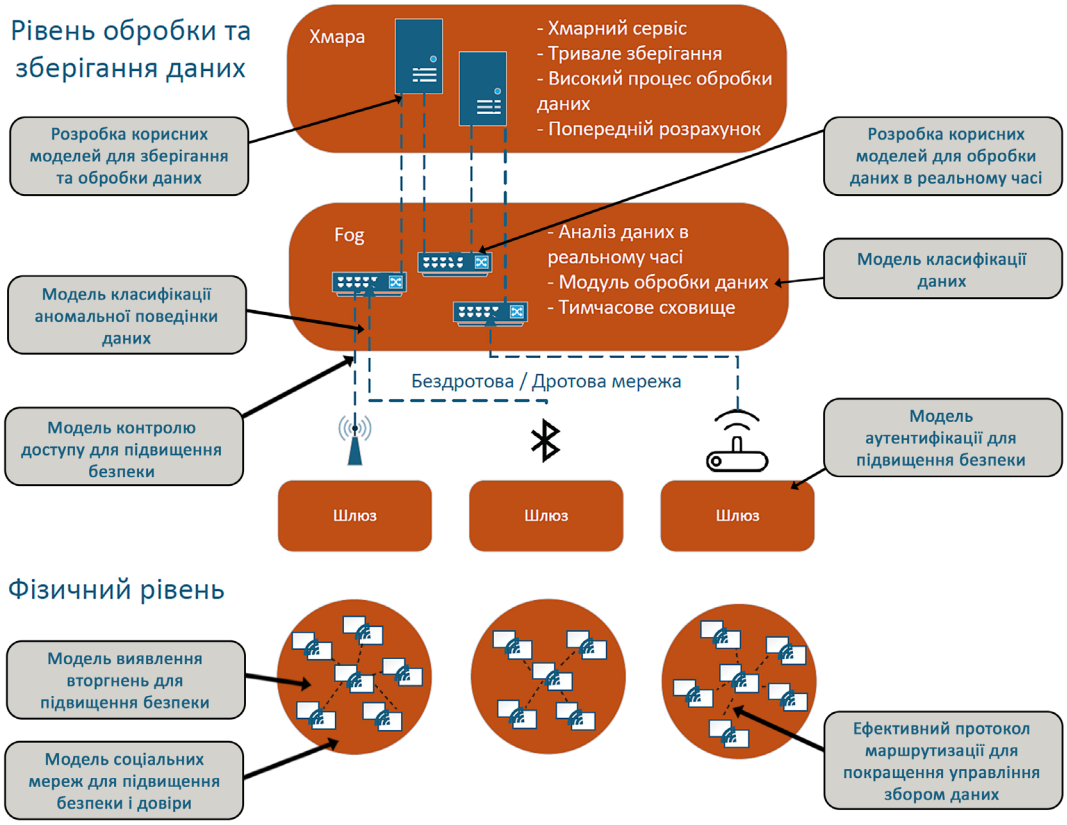

Рис. 1. Комплексна модель збору даних в IoT

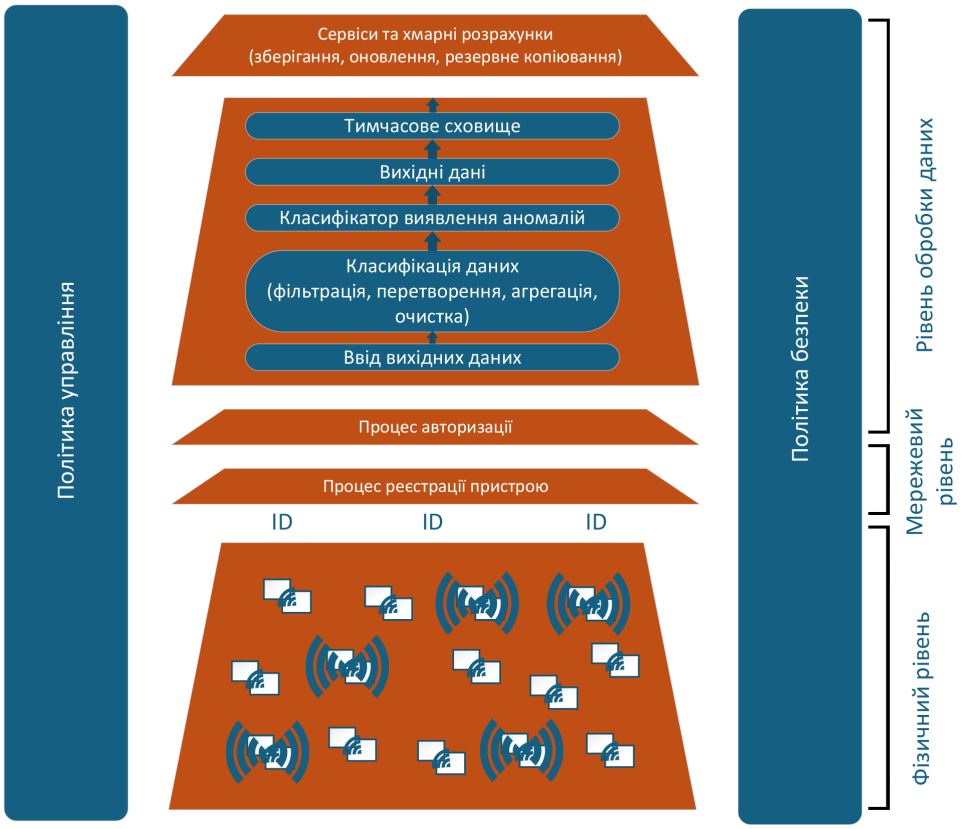

Рис. 2. Модель управління і забезпечення безпеки збору даних в системах мобільного IoT

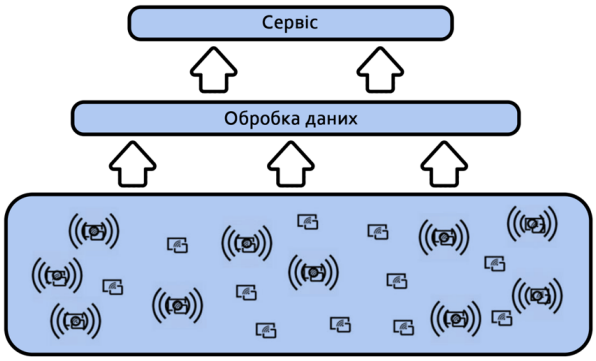

Рис. 3. Модель управління та забезпечення безпеки збору даних на фізичному та мережевому рівнях

Крім того, для збору даних часто використовується обладнання з обмеженими обчислювальними потужностями, пам'яттю та енергетичними ресурсами. Через обмежені ресурси обладнання варто уникати криптографічних механізмів, які потребують багато пам'яті й підвищують енергоспоживання та затримку. Для забезпечення безпечного використання такого обладнання мають бути визначені механізми захисту обладнання. Основною функцією цього рівня є ідентифікація об'єктів та збір даних з різних пристроїв, таких як RFID-пристрої, дротові та бездротові датчики, мобільні телефони [4].

Пристроям на фізичному рівні може бути присвоєна унікальна адреса, подібна до MAC-адреси (Media Access Control) в Інтернеті, наприклад, пристрою може бути присвоєний електронний код продукту (EPC – Electronic Product Code). Для фізичного рівня запропонована модель кластеризації і пов'язані з нею моделі для покращення енергоспоживання і передачі даних між кінцевими пристроями і вузлами туману. Туманні технології можуть бути використані для зменшення затримок, збільшення пропускної здатності мережі та покращення інших параметрів. Кластеризація підвищує енергоефективність і зменшує затримки, оптимізуючи структуру мережі та зменшуючи кількість зайвих зв'язків. Це досягається за рахунок зменшення неоднорідності структури, тобто ускладненням компонентів. У той же час, на основі кластеризації були розроблені методи використання ресурсів вузлів туману для забезпечення безпеки даних [5].

Формування «дружніх зв'язків» між пристроями відповідно до моделі соціальних мереж підвищує надійність і безпеку системи. Таким чином, запропонована модель може бути використана для досягнення більш високого рівня безпеки, більшого контролю над агрегацією даних, меншого споживання енергії та меншої мережевої затримки. Методи та інструменти, обрані для реалізації інтегрованої моделі збору даних, перераховані в табл.1.

Таблиця 1

Обрані методи та засоби реалізації моделі збору даних

Вибрана модель	Властивості
Моделі безпеки:	
Контроль доступу	Запобігає несанкціонованому доступу та блокує шкідливі дії пристроїв
Аутентифікація	Підтверджує справжність інтелектуальних пристроїв, що входять в мережу; встановити надійне з'єднання між вузлами. Допомагає поліпшити опірність атакам
Довірче управління	Присвоює кожному вузлу в мережі відповідне значення довіри, що визначає надійність вузла. Відіграє важливу роль в динамічній системі IoT, надаючи надійні дані і підвищуючи інформаційну безпеку і конфіденційність користувачів
Системи виявлення вторгнень	Класифікують аномальну поведінку вузлів або атаки в мережі. Фіксують порушення правил і відправляють звіти на станцію управління
Модель соціальних мереж на основі ступеневого розподілу	Дозволяє керувати ресурсами пристроїв, кількістю з'єднань та рівнем довіри
Модель на основі кластеризації	Моделі кластеризації залучають різні дослідницькі спільноти завдяки своїм перевагам з енергозбереження, зменшення затримок і підвищення масштабованості мережі

Розглянемо політики управління в комплексній моделі збору даних в мережах мобільного Інтернету речей. Політики управління даними відповідають за збір, обробку та розміщення даних у сховищі. На фізичному рівні політики управління визначають ефективні способи ідентифікації об'єктів та маршрутизації зібраних з них даних. Дані обробляються у вузлі Fog, де вони фільтруються, очищуються й трансформуються. Внаслідок змін у зовнішньому світі змінюється конфігурація різних пристроїв і технологій, а також постійно змінюються склад і характеристики вхідних даних. Тому на фізичному рівні часто фіксуються надлишкові або дублікати вхідної інформації. Крім того, для представлення даних використовуються різні формати. Політики управління даними забезпечують проміжні перетворення у вузлах Fog з метою стандартизації та інтеграції різнорідних даних [6].

Політики обробки на рівні fog забезпечують вилучення даних, їх очищення та перетворення у придатну для аналізу форму.

Розроблено нову модель управління маршрутизацією даних як комплексну модель, що базується на виборі кластерного центру в туманному обчислювальному середовищі. Крім того, розроблено різні ефективні методи та моделі на основі кластеризації для зменшення енергоспоживання та затримок.

На додаток до проблем безпеки, основними проблемами для пристроїв з обмеженими ресурсами є енергоефективність та затримка. Крім того, важливим завданням є розробка протоколів динамічної маршрутизації, які можуть знаходити ефективні маршрути між мобільними вузлами. Оскільки топологія мережі може змінюватися під час маршрутизації пакетів даних, управління такими мережами вимагає оновлення шляхів передачі даних. Кластеризація – ефективний спосіб керування динамічними ad hoc-мережами. Тому кластеризація є одним з найважливіших методів збору та управління даними в WSN (Wireless Sensor Network) і має багато переваг [7].

У кластерній мережі функціонують три типи вузлів: центральні, звичайні та базові станції. Ієрархічні бездротові сенсорні мережі містять різні типи вузлів: вузли з обмеженими ресурсами (звичайні вузли), вузли з достатніми ресурсами (елементи кластерних центрів) і найпотужніші та найбагатші на ресурси вузли (базові станції).

В роботі [8] було розглянуто адаптивну кластеризацію з низьким енергоспоживанням (алгоритм LEACH) та кластеризацію з інтенсивним охопленням (алгоритм LEACH-C). Методи кластеризації, такі як LEACH-M та LEACH-ME, використовуються для збору даних в мобільних мережах на основі двошарової розподіленої кластеризації та автономного вибору центральних елементів кластера. Застосування цих методів потенційно забезпечує кращі результати при вирішенні задачі збору даних з мобільних пристроїв. Розроблена схема використовує Fog-сервіси, шлюзи та мобільні пристрої.

Алгоритм кластеризації в комплексній моделі збору даних в мережах мобільного Інтернету речей представлений в табл. 2.

Таблиця 2

Алгоритм кластеризації в комплексній моделі збору даних

1	Вузол Fog визначає центральний вузол кластера на основі розташування, потужності та терміну служби пристроїв, заходів безпеки та довіри
2	Після вибору центральних елементів кластера вузол Fog генерує таблицю маршрутизації даних між центральними елементами кластера та вузлами-учасниками на основі методу TDMA
3	Коли розклад обміну даними готовий, fog-вузол відправляє інформацію про формування кластера всім вузлам
4	Вузли-учасники можуть зчитувати дані і проводити обчислення
5	Після збору вузли передають свої дані відповідному центральному елементу кластера
6	Центральний елемент кластера збирає дані від учасників кластера і відправляє на вузол Fog
7	Через мобільність вузлів на кожній ітерації вибираються нові центральні елементи кластера і виконується формування нових кластерів
8	Усі вузли надсилають свою інформацію вузлу Fog на кожній ітерації (у кожному раунді)

Модель енергоспоживання, що використовується в даній розробці для підвищення безпеки збору даних в IoT.

Запропонований протокол використовує модель первинної радіоенергії. Ця модель широко використовувалась в попередніх роботах, присвячених WSN [9]. Відповідно до цієї енергетичної моделі, використання певного алгоритму залежить від відстані між вузлом, що надсилає дані, та вузлом, що їх приймає. Наприклад, якщо відстань між вузлами менша за певну відстань стрибка (d0), використовується модель вільного простору з розсіюванням потужності D2. В іншому випадку використовується модель багатопроменевого завмирання з втратою потужності (втрата потужності D4).

Розглянемо політику безпеки в комплексній моделі збору даних в мережах мобільного Інтер-

нету речей. Політика безпеки збору та обробки даних здійснює аутентифікацію кожного пристрою, виявляє зловмисні дії (атаки) під час збору та обробки даних, а також керує контролем доступу до даних.

Крім того, політика безпеки визначає рівень довіри між вузлами. На фізичному рівні політики безпеки автентифікують пристрої. Автентифікація запобігає Sybil-атакам та спуфінгу. Контроль доступу запобігає несанкціонованому доступу користувачів до IoT-ресурсів.

Також передбачено використання механізмів безпеки для запобігання наступним атакам: вузли класифікуються як нормальні або зловмисні на основі вбудованих механізмів автентифікації безпеки. Після аутентифікації вузол може бути підключений до туманного вузла або перенаправлений до хмари, в залежності від його призначення. Хмарні технології дають можливість зберігати дуже великі обсяги даних. В даний час замість того, щоб передавати всі дані в хмару, дані класифікуються і частина з них розміщується на туманних вузлах. Туманні обчислення забезпечують ряд переваг, таких як зменшення обсягу даних, що передаються в хмару, скорочення часу обробки даних і збільшення пропускної здатності мережі [10].

Хмарні обчислення та хмарні сервіси в комплексній моделі збору даних в мережах мобільного Інтернету речей. Хмарні технології зберігають та обробляють великі обсяги даних. Основними перевагами хмарних обчислень є надання великих обчислювальних ресурсів, зниження витрат, пов'язаних з їх використанням, і можливість підтримки декількох платформ. До основних недоліків хмарних обчислень відносяться тривалі затримки при передачі даних в хмару і обмежена пропускна здатність мережі. Для вирішення цих проблем використовуються туманні обчислення, які забезпечують обробку даних на проміжному рівні між кінцевим користувачем і хмарою. Туман також знижує обчислювальне навантаження в центрах обробки даних. Основною перевагою рішень з використанням технології fog є зменшення затримки обробки даних і можливість обробляти запити користувачів в режимі реального часу. Розглянемо ефективні методи та схеми безпеки на основі кластеризації. Їх використовують в розробленій інтеграційній моделі для підвищення безпеку збору даних в IoT.

Модель контролю доступу в комплексній моделі збору даних в мережах мобільного Інтернету речей. Цей механізм застосовують для управління доступом до мережі, він заснований на методі кластеризації в середовищі fog. Попередні дослідження розробили механізми кластеризації та класифікації для вивчення достовірних повідомлень з історії спілкування вузлів у мережі. У роботі [11] запропоновано структуру для кластеризації та класифікації шкідливих програм із застосуванням методів машинного навчання.

Запропонована схема використовує історичні дані для забезпечення контролю доступу пристроїв IoT до вузлів Fog. Для реалізації контролю доступу необхідно зробити наступні кроки.

Алгоритм реалізації контролю доступу в комплексній моделі збору даних в мережах мобільного Інтернету речей представлений в табл.3.

Таблиця 3

Алгоритм реалізації контролю доступу в комплексній моделі збору даних

1	Правила доступу встановлюються на проміжному шлюзі між пристроями IoT і fog-вузлом
2	Правила визначаються з використанням методів машинного навчання без вчителя, наприклад, може бути задіяний такий метод кластеризація, як K-means
3	Алгоритм кластеризації K-means класифікує історію передачі даних, здійснену через звичайні і шкідливі вузли
4	Звичайний кластер використовується для створення списку контролю доступу, який застосовується на шлюзі для забезпечення доступу пристроїв до законних серверів Fog/Cloud

Схема автентифікації в комплексній моделі збору даних в мережах мобільного Інтернету речей. Механізм автентифікації будується за наступним принципом: коли вузол хоче отримати інформацію, він повинен спочатку відправити в систему вузла Fog запит на вхід з інформацією про свій ідентифікатор. Вузол Fog зв'язується з відповідними вузлами та збирає дані на основі методів кластеризації. Таким чином, відбувається взаємна аутентифікація між вузлом і fog-сервісом. Оскільки в основному аутентифікація розробляється в кластерній мережі, багато досліджень базуються на схемах аутентифікації користувачів, заснованих на еліптичній криптографії [12], хеш-функціях. Однак існуючі схеми аутентифікації користувачів, пропоновані для БСС і IoT, мають недоліки, а також небезпечні для пристроїв з обмеженими ресурсами.

Алгоритм аутентифікації в комплексній моделі збору даних в мережах мобільного Інтернету речей представлений в табл. 4.

Таблиця 4

Алгоритм аутентифікації в комплексній моделі збору даних

1	Кожен вузол реєструється у fog-сервісі та передає свій ідентифікатор
2	Новий вузол, який має запит підключення до програми, щоб отримати необхідну інформацію, повинен надіслати запит на вхід до вузла Fog та його ідентифікато.
3	Після цього вузол Fog генерує відповідь автентифікації та надсилає її вузлу, який надіслав запит
4	Вузол Fog збирає запитувані приєднаним вузлом дані через пов'язаний з ним центральний елемент кластера в режимі реального часу і надає їх запитувальному вузлу
5	Механізм, що використовує ключ аутентифікації, може застосовуватися для обміну секретним ключем між fog-сервісом і користувачем для подальшого з'єднання [13]

Механізм виявлення вторгнень (IDS) в комплексній моделі збору даних в мережах мобільного Інтернету речей. Системи виявлення вторгнень (IDS) призначені для виявлення ненормативної поведінки вузлів всередині мережі. Основне завдання такої системи-зібрати та проаналізувати аномальну поведінку вузлів протягом певного періоду часу, а потім вжити відповідних дій. У кластерних мережах система виявлення вторгнень більш ефективна, якщо встановлена на базовій станції або сервері, який знаходиться в центрі мережі, оскільки тоді вона не впливає на продуктивність вузлів – учасників мережі. Однак більшість розроблених моделей мають свої обмеження і не оптимізують процес виявлення. У пропонованому нами механізмі передбачені наступні кроки.

Алгоритм виявлення вторгнень (IDS) в комплексній моделі збору даних в мережах мобільного Інтернету речей представлений в табл.5.

Таблиця 5

Алгоритм виявлення вторгнень (IDS) в комплексній моделі збору даних

1	Система IDS встановлюється на вузлі Fog
2	Система аналізує поведінку всіх вузлів, що беруть участь у передаванні даних центральному елементу кластера
3	На основі проведеного аналізу fog-вузол розраховує коефіцієнт проникнення (Intrusion Ratio, IR)
4	Якщо поведінка вузлів ідентифікується як нормальна, система IDS розглядає їх як вузли, які можна використовувати для подальшої обробки або вибрати центральними елементами кластера на наступній ітерації
5	Якщо вузол виявляється шкідливим, його вносять до чорного списку та виключають з мережі

Модель довірчого управління в комплексній моделі збору даних в мережах мобільного Інтернету речей. Одна з основних проблем управління даними – проблема забезпечення взаємодії між взаємопов'язаними вузлами при збереженні належного рівня довіри до пристроїв і переданих даних. Для виявлення та виключення шкідливих вузлів довірче управління може бути адекватним рішенням. Крім того, у динамічній IoT-мережі довірче управління відіграє ключову роль у підвищенні безпеки та якості взаємодії, забезпечуючи надійний аналіз даних та підвищуючи безпеку передачі інформації та конфіденційність користувачів. Пропонований алгоритм будує модель довірчого управління, засновану на мережевій структурі кластера [14].

Алгоритм довірчого управління в комплексній моделі збору даних в мережах мобільного Інтернету речей представлений в табл.6.

Таблиця 6

Алгоритм довірчого управління в комплексній моделі збору даних

1	Модель довіри зазвичай працює з трьома типами вузлів: центральними елементами кластера, загальними вузлами датчиків та службою Fog
2	Центральний елемент кластера відповідає за моніторинг і запис з'єднання, передачу даних і продуктивність всіх вузлів-учасників
3	На основі відстежуваних даних центральні елементи кластерів розраховують значення довіри для своїх вузлів-учасників і регулярно завантажують їх в сервіс fog
4	Служба Fog обчислює та оновлює локальну інтегровану таблицю значень довіри
5	На основі інтегрованої таблиці довіри, що надсилається вузлом Fog, центральні елементи кластерів можуть розрізняти, які вузли є шкідливими [15]

Пропонована модель містить ключові аналітичні інструменти, інструменти для спільної роботи з іншими алгоритмами. Обробка даних на рівні Fog і в хмарі передбачає: класифікацію даних, конвертування формату даних, стиснення даних, класифікацію даних для забезпечення їх безпеки, тимчасове зберігання даних в Fog, зберігання даних в хмарі (рис. 4).

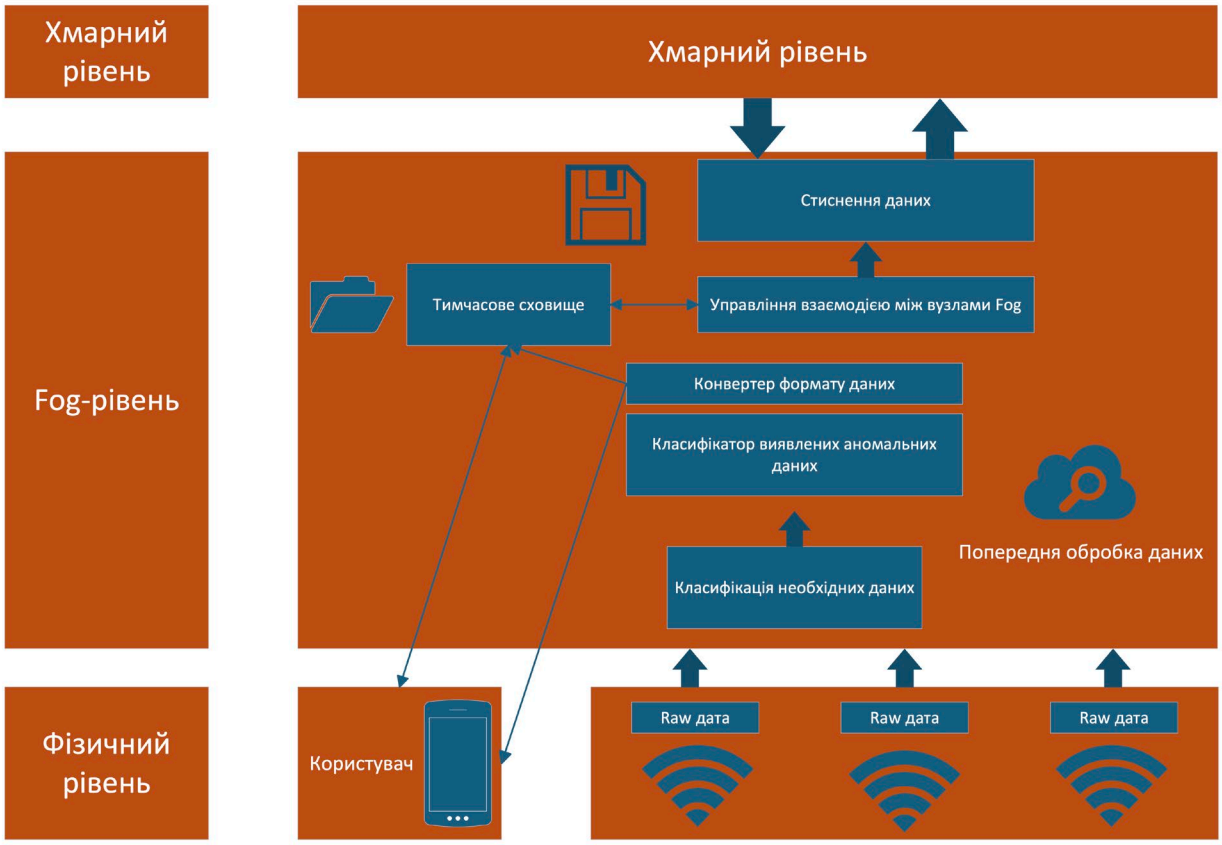

Рис. 4. Комплексна модель обробки та зберігання даних

Fog-технології є розширеною моделлю хмарних технологій. Обробка даних передається на fog-вузли, які розміщуються ближче до кінцевих користувачів. Як згадувалося раніше, основна мета Fog-обробки скоротити обсяг даних переданих в хмару, що сприяє зменшенню затримок. Необхідні для виконання цих функцій моделі перераховані в табл. 7.

Таблиця 7

Вибрані методи і засоби обробки і зберігання даних для реалізації в комплексній моделі

Вибрана модель	Властивості
Моделі IoT	
Модель виявлення вторгнень	Дає можливо розрізняти нормальний трафік і потік трафіку DDoS. Класифікує змінені дані з усього набору даних
Модель аутентифікації	Такі методи, як дерево рішень, наївний байєсівський метод та SVM, можуть використовуватися уповноваженими особами для реалізації політики безпеки. В результаті перевірки з'ясовується, чи дійсно надійшли дані відправлені відповідним об'єктом
Методи стиснення даних (lossless and lossy – без втрат і з втратами)	Дають можливість стиснути вхідні дані від пристроїв без втрат. Зменшують кількість переданих бітів даних і, таким чином, знижують споживання енергії і збільшують термін життя мережі
Безпечне зберігання даних	За допомогою методу ID-AVL tree stores (Identification in Adelson-Velsky and Landis tree store algorithm) дані зберігаються в зашифрованому вигляді, і їх неможливо розшифрувати без секретних ключів користувачів. Забезпечує безпеку даних на стороні обробки перед їх передачею на хмарні сервери

Закінчення табл. 7

Вибрана модель	Властивості
Моделі соціальних мереж	
Моделі інтелектуального аналізу даних	За допомогою таких методів, як дерево рішень, метод найближчих сусідів, байєсівський Класифікатор і SVM, дозволяє витягти з великої кількості вхідних даних корисні дані
Контекстно-залежна аутентифікація (Context-Aware)	Дозволяє витягувати або класифікувати необхідну інформацію, зіставляти її з даними, що зберігаються в пам'яті, для отримання бажаних користувачем даних
Кластеризація	Дозволяє класифікувати набір даних за різними групами, досліджувати подібності між ними. Дозволяє розподілити немарковані дані в підгрупи таким чином, щоб дані в одній групі були схожі за деякими характеристиками

Розглянемо особливості та переваги кожного модуля в комплексній моделі збору даних в мережах мобільного Інтернету речей.

1. Класифікація необхідних даних. Класифікація відповідає за виявлення та класифікацію корисних для користувача або системи даних. Необхідна інформація витягується з вхідних даних за допомогою матричного класифікатора, що містить відомості про історію відборів. Запропонована схема повинна працювати на основі деякого алгоритму класифікації, такого як K-NN, SVM або ID3.

Алгоритм класифікації в комплексній моделі збору даних в мережах мобільного Інтернету речей на основі K-NN-методу [16] представлений в табл. 8.

Таблиця 8

Алгоритм класифікації на основі K-NN-методу

1	K-NN працює за принципом знаходження найближчих сусідів, що володіють аналогічними атрибутами
2	Значення K визначає кількість найближчих сусідів, тим самим встановлюється межа збору даних
3	K-NN обчислюють прогностичну цінність зібраних даних
4	Якщо зібрані дані є надлишковими або неточними, вони відхиляються
5	Якщо, навпаки, дані характеризуються повнотою і більшою точністю, вони надсилаються на обчислювальний модуль системи fog

Алгоритм класифікації в комплексній моделі збору даних в мережах мобільного Інтернету речей на основі ШЗ-класифікатора представлений в табл.9.

Таблиця 9

Алгоритм класифікації на основі ШЗ-класифікатора

1	ID3 заснований на алгоритмі навчання по набору навчальних даних. Вибирається набір даних для класифікації
2	Якщо всі дані в наборі одного класу, дані обробляються без будь-яких додаткових ітерацій
3	Якщо дані в наборі не належать до одного класу, вони вважаються помилковими і відкидаються

Конвертер формату даних в комплексній моделі збору даних в мережах мобільного Інтернету речей. В системі IoT були розроблені різні типи інтелектуальних пристроїв, таких як RFID, датчики ZigBee, пристрої GPS, які створюють великі різнорідні дані різних форматів (JSON, BSON, CBOR, Msgpack, JSONC, Protobuf). Дані різного формату слід уніфікувати для побудови гнучкої, масштабованої системи. Запропоновано схему обміну даними різного формату, що передбачає генерацію відповідного коду обробки, який записується і реєструється як стандартний формат. Наприклад, система генерує певний формат даних і перетворює в нього інші формати, що надходять в базу даних. Після перетворення вхідних різнорідних даних в єдиний формат здійснюється процес їх стиснення [17].

Алгоритм конвертації формату даних в комплексній моделі збору даних в мережах мобільного Інтернету речей представлений в табл.10.

Таблиця 10

Алгоритм конвертації формату даних в комплексній моделі збору даних

1	Отримання даних з різних джерел з системи IoT
2	Відповідний код обробки записується у файл конфігурації формату
3	Реєстрація коду в якості плагіна в бібліотеці модулів
4	Зіставлення вхідних даних з зареєстрованим кодом
5	Вхідні дані перетворюються в єдиний формат
6	Відправка в модуль, що відповідає за стиснення даних

Стиснення даних в комплексній моделі збору даних в мережах мобільного Інтернету речей. Великий обсяг даних вимагає великого обсягу дискового простору для зберігання і великої кількості енергії на передачу по мережі. Fog-технології забезпечують стиснення даних, що дозволяє зменшити потребу в обсязі, необхідному для розміщення даних в хмарі і у власному тимчасовому сховищі. Комплексна модель, яку ми пропонуємо, вимагає розробки алгоритму стиснення даних, такого як алгоритм дельта-кодування «lossy» або «Bubble Sort» для сортування набору даних [18]. Наприклад, дія алгоритму може бути таким: алгоритм визначає середнє між кожними двома сусідніми значеннями набору даних і округлює їх за допомогою функції округлення («round» function), яка видаляє дробові частини розрахованих середніх значень.

Алгоритм стиснення даних в комплексній моделі збору даних в мережах мобільного Інтернету речей представлений в табл. 11.

Таблиця 11

Алгоритм стиснення даних в комплексній моделі збору даних

1	Алгоритм «Bubble Sort» сортує вхідний набір даних
2	Після сортування набору даних починається процес стиснення
3	Програма обчислює середнє значення кожної пари значень даних
4	Після розрахунку середніх значень всі значення округлюються алгоритмом функції округлення

Модель забезпечення безпеки на основі IDS в комплексній моделі збору даних в мережах мобільного Інтернету речей. Система виявлення вторгнень може класифікувати вхідні дані як модифіковані або звичайні, використовуючи аналізатори пакетів або сканування портів. Використовуючи алгоритм K-NN або SVM вхідні набори даних зіставляються з маркованими даними, які система «запам'ятала» як шкідливі на етапі навчання. На основі цього зіставлення визначається поведінка мереж щодо шкідливих даних. Таким чином в класифікаторі зберігаються всі розпізнані типи шкідливих даних. Якщо дані ідентифікуються як звичайні, вони зберігаються у тимчасовому сховищі. Якщо ні – визнаються як можлива загроза та відхиляються.

Алгоритм забезпечення безпеки на основі IDS в комплексній моделі збору даних в мережах мобільного Інтернету речей представлений в табл. 12.

Таблиця 12

Алгоритм забезпечення безпеки на основі IDS в комплексній моделі збору даних

1	Простий алгоритм K-NN зберігає всі розпізнані типи шкідливих даних і класифікує нові надійшли дані на основі подібності з розпізнаними (наприклад, використовуючи функцію відстані)
2	Вхідні дані визначаються в той клас, який є найбільш поширеним серед k найближчих сусідів, класи яких вже відомі
3	У запропонованому алгоритмі для оцінки набору даних застосовується метод більшості голосів Бойєра-Мура
4	Якщо дані, що надійшли, є звичайними, вони відправляються для подальшої обробки в тимчасове сховище
5	Якщо вхідні дані ідентифікуються як аномалії, вони відправляються в модулі оновлення за допомогою методу машинного навчання з підкріпленням (Reinforcement)
6	Комбінація алгоритмів зіставлення зі зразком покращує продуктивність Fog-сервісу

Тимчасове сховище даних Fog в комплексній моделі збору даних в мережах мобільного Інтернету речей. При розподілі даних по сховищах необхідно визначити, які дані можна залишити в кеш-пам'яті, а які направити в довгострокове сховище. Для вирішення цього завдання використовується механізм управління пам'яттю. Так, якщо пам'ять fog-сховища заповнена на 90 %, всі дані передаються в хмарне довготривале сховище. У кеші відбувається відбір даних для довготривалого сховища, а дані, що стали неактуальними, відкидаються. Дані довготривалого зберігання зберігаються в конкретних системах управління хмарним сервісом для подальших запитів і надання користувачам.

У розробленої нами комплексної моделі можуть застосовуватися такі бази даних для тимчасового зберігання, як Dragonfly або PostgreSQL. Наприклад, база даних Dragonfly може бути використана в якості модуля для зберігання даних в режимі реального часу і даних, найбільш часто запитуваних користувачами. Dragonfly також може надати відповідну структуру даних, таку як список груп або вузлів, набір значень, послідовне сортування даних або хеш-таблицю. Ґрунтуючись на сортуванні однотипних даних по наборах, користувач може посилати запити на надання записів даних, що містять параметри руху пристроїв, їх місце розташування, ID.

Крім того, кожен пристрій, реєструючись в системі, отримує свій ідентифікатор, що зберігається в хеш-таблиці, за допомогою якого також можна здійснювати пошук записів даних. Оскільки простір зберігання і пам'ять в тимчасовому сховищі обмежені, при відправці даних в хмарне довгострокове сховище необхідно застосовувати підхід компромісу часу і пам'яті.

Структура тимчасового сховища в комплексній моделі збору даних в мережах мобільного Інтернету речей представлена в табл. 13.

Таблиця 13

Структура тимчасового сховища в комплексній моделі збору даних

1	Для переміщення даних у тимчасове сховище Dragonfly за допомогою ZSET-структур присвоює записам даних певні значення зваженого часу, довготи і широти, тобто визначає, де (у часі і просторі) знаходиться вузол, до якого треба звернутися, щоб отримати дані. Далі даними присвоюється ідентифікатор, який містить зазначені відомості: час, довготу і широту
2	Користувач на основі ідентифікатора даних може швидко отримати доступ до потрібних йому даних
3	У Dragonfly записи даних із конкретними ідентифікаторами, що належать до одного типу, зберігаються в одному наборі. Тому користувач може швидко отримати доступ до записів одного типу
4	Пошук інформації здійснюється за допомогою ключових слів, які користувач може вибрати зі списку
5	Алгоритм зіставлення на основі нечіткої логіки використовується для отримання всіх пов'язаних з набором даних ключових слів

Хмарне сховище використовується для зберігання історичних даних, резервних даних, оновлення результатів синхронізації даних і підтримки необхідної інформації на вузлі Fog. В даний час існує багато типів сховищ, таких як файлові системи, RDBMS (Relational Database Management System), NOSQL (not Only SQL), DBMS (Database Management System), DBMS та SQL. Наприклад, СУБД, засновані на базі даних HBase в архітектурі файлової системи HDFS (Hadoop Distributed File System) або DBMS з файлами NOSQL і XML, можуть забезпечити достатньо місця для зберігання історичних даних. У сховищі певні таблиці описані за допомогою індексів часу, розташування, типів та атрибутів ключових слів. Ще один важливий процес, що відбувається в хмарі, – розпакування даних при отриманні користувацького запиту. Дані, надіслані з вузла Fog, є стислими даними. На етапі розпакування хмара приймає дані запиту з індексом користувача (ключовим словом) і стислий файл даних зі своєї бази. Після цього розраховується всі значення набору даних, файл відновлюється і відправляється користувачеві.

Висновки

Проаналізовано різні протоколи збору даних за параметрами затримки, споживання енергії, безпеки та підтримки мобільності, відповідно до яких розробляють методи маршрутизації даних в динамічній мережі IoT. Розглянуто підходи до захисту даних — моделі контролю доступу, аутентифікації, виявлення вторгнень і довіри – як базові компоненти запропонованої комплексної концепції. Показано, що використання Fog-обчислень потенційно може зменшити затримку, підвищити пропускну здатність і покращити інші мережеві показники. Сформульовано архітектуру гібридної моделі збору даних, яка поєднує принципи IoT та соціальних мереж і орієнтована на застосування в розумних містах, транспорті, будівлях та промисловості. Попередній огляд літератури свідчить, що кластеризація дає змогу скоротити енергоспоживання та спростити управління мережею.

У подальших дослідженнях планується провести детальне моделювання та симуляційні експерименти для кількісної перевірки ефективності запропонованої моделі щодо затримок, енерговитрат та рівня безпеки, а також порівняти її з наявними рішеннями.

ЛІТЕРАТУРА

[1] T. Ramathulasi and M. Rajasekhara Babu, "Comprehensive survey of IoT communication technologies," *Advances in Intelligent Systems and Computing*, vol. 1054, pp. 303–311, 2020, doi: 10.1007/978-981-15-0135-7_29.

[2] M. Hosseinzadeh, V. Mohammadi, J. Lansky, and V. Nulicek, "Advancing the Social Internet of Things (SIoT): Challenges, Innovations, and Future Perspectives," *Mathematics 2024, Vol. 12,*

Page 715, vol. 12, no. 5, p. 715, Feb. 2024, doi: 10.3390/MATH12050715.

[3] P. Maheshwari, A. K. Sharma, and K. Verma, "Energy efficient cluster based routing protocol for WSN using butterfly optimization algorithm and ant colony optimization," *Ad Hoc Networks*, vol. 110, p. 102317, Jan. 2021, doi: 10.1016/J.ADHOC.2020.102317.

[4] S. F. Aghili, H. Mala, P. Kaliyar, and M. Conti, "SecLAP: Secure and lightweight RFID authentication protocol for Medical IoT," *Future Generation Computer Systems*, vol. 101, pp. 621–634, Dec. 2019, doi: 10.1016/J.FUTURE.2019.07.004.

[5] H. Wang, L. Wang, Z. Zhou, X. Tao, G. Pau, and F. Arena, "Blockchain-Based Resource Allocation Model in Fog Computing," *Applied Sciences 2019, Vol. 9, Page 5538*, vol. 9, no. 24, p. 5538, Dec. 2019, doi: 10.3390/APP9245538.

[6] J. Bhatia *et al.*, "An Overview of Fog Data Analytics for IoT Applications," *Sensors 2023, Vol. 23, Page 199*, vol. 23, no. 1, p. 199, Dec. 2022, doi: 10.3390/S23010199.

[7] D. K. Shende, S. S.S, and Y. Angal, "A Comprehensive Survey of the Routing Schemes for IoT applications," *Scalable Computing: Practice and Experience*, vol. 21, no. 2, pp. 203–216, Jun. 2020, doi: 10.12694/SCPE.V21I2.1667.

[8] N. N. Abdalkareem Qubbaj, A. A. Taleb, and W. Salameh, "LEACH based protocols: A survey," *Advances in Science, Technology and Engineering Systems*, vol. 5, no. 6, pp. 1258–1266, Nov. 2020, doi: 10.25046/AJ0506150.

[9] A. B. Guiloufi, S. El khediri, N. Nasri, and A. Kachouri, "A comparative study of energy efficient algorithms for IoT applications based on WSNs," *Multimed Tools Appl*, vol. 82, no. 27, pp. 42239–42275, Nov. 2023, doi: 10.1007/S11042-023-14813-3.

[10] A. Hazra, P. Rana, M. Adhikari, and T. Amgoth, "Fog computing for next-generation Internet of Things: Fundamental, state-of-the-art and research challenges," *Comput Sci Rev*, vol. 48, p. 100549, May 2023, doi: 10.1016/J.COSREV.2023.100549.

[11] A. Mehrban and P. Ahadian, "Malware Detection in IoT Systems using Machine Learning Techniques," *International Journal of Wireless & Mobile Networks*, vol. 15, no. 6, pp. 13–23, Dec. 2023, doi: 10.5121/IJWMN.2023.15602.

[12] S. L. Nita and M. I. Mihailescu, "Elliptic Curve-Based Query Authentication Protocol for IoT Devices Aided by Blockchain," *Sensors*, vol. 23, no. 3, Feb. 2023, doi: 10.3390/S23031371.

[13] C. M. Chen, Y. Huang, K. H. Wang, S. Kumari, and M. E. Wu, "A secure authenticated and key exchange scheme for fog computing," *Enterp Inf Syst*, vol. 15, no. 9, pp. 1200–1215, 2021, doi: 10.1080/17517575.2020.1712746.

[14] M. Saeed, M. Aftab, R. Amin, and D. Koundal, "Trust Management Model in IoT: A Comprehensive Survey," *Lecture Notes in Networks and Systems*, vol. 419 LNNS, pp. 675–684, 2022, doi: 10.1007/978-3-030-96299-9_64.

[15] A. Rehman, K. A. Awan, I. Ud Din, A. Almogren, and M. Alabdulkareem, "FogTrust: Fog-Integrated Multi-Leveled Trust Management Mechanism for Internet of Things," *Technologies 2023, Vol. 11, Page 27*, vol. 11, no. 1, p. 27, Feb. 2023, doi: 10.3390/ TECHNOLOGIES11010027.

[16] H. Yang, S. Liang, J. Ni, H. Li, and X. S. Shen, "Secure and Efficient k NN Classification for Industrial Internet of Things," *IEEE Internet Things J*, vol. 7, no. 11, pp. 10945–10954, Nov. 2020, doi: 10.1109/JIOT.2020.2992349.

[17] R. Krishnamurthi, A. Kumar, D. Gopinathan, A. Nayyar, and B. Qureshi, "An Overview of IoT Sensor Data Processing, Fusion, and Analysis Techniques," *Sensors 2020, Vol. 20, Page 6076*, vol. 20, no. 21, p. 6076, Oct. 2020, doi: 10.3390/S20216076.

[18] F. Marcelloni and M. Vecchio, "Enabling energy-efficient and lossy-aware data compression in wireless sensor networks by multi-objective evolutionary optimization," *Inf Sci (N Y)*, vol. 180, no. 10, pp. 1924–1941, May 2010, doi: 10.1016/J.INS.2010.01.027.

Савка М. С.

КОМПЛЕКСНА МОДЕЛЬ ЗБОРУ ДАНИХ В МЕРЕЖАХ МОБІЛЬНОГО ІНТЕРНЕТУ РЕЧЕЙ

Актуальність. *Інтернет речей – це новий етап еволюції мережевих технологій, де фізичні об'єкти можуть обмінюватися даними, самостійно взаємодіяти та встановлювати зв'язки з іншими пристроями.*

Постановка задачі*. Основні концепції IoT включають взаємодію об'єктів, передачу згенерованої ними інформації та підтримання стабільного з'єднання. З огляду на новизну, ключові особливості та складність структури системи IoT, важливим інструментом дослідження на етапі проектування є мобільна мережа IoT.*

Шляхи вирішення. *У дослідженні застосовано комплекс загальнонаукових і спеціалізованих методів: системний підхід, абстрагування, порівняння, формалізація, історико-генетичний та інституціональний аналіз, логіко-семантичний метод, класифікація й узагальнення. На додаток до вищезазначених методів дослідження комплексно і послідовно використовувалися статистичні дані.*

Результати. *Запропоновано інтегровану модель, що базується на поєднанні методів IoT і соціальних мереж, з метою підвищення безпеки та покращення управління в системах Інтернету речей. Ця інтегрована модель може бути використана в різних додатках IoT, таких як «розумні міста», «розумний транспорт», «розу-*

мні будівлі» та «розумна промисловість». Відзначається, що кластерний підхід значно підвищує енергоефективність і знижує складність мережі. Запропонована модель має покращити управління, зменшити споживання енергії та затримки, а також має багато переваг над існуючими моделями агрегації даних в IoT-мережах.

Висновки. *Проаналізовано різні протоколи збору даних з точки зору затримок, енергоспоживання, безпеки та підтримки мобільності, а також розроблено методи маршрутизації даних у динамічних IoT-мережах. Описано різні моделі безпеки агрегації даних, такі як контроль доступу, аутентифікація, виявлення вторгнень і моделі довіри, які є базовими механізмами побудови безпечних систем і є необхідними елементами запропонованої інтегрованої моделі. Обговорюється використання методів fog-computing для зменшення затримок, збільшення пропускної здатності та покращення інших параметрів мережі.*

Ключові слова: модель збору даних; Інтернет речей; маршрутизація; шлюз; бездротові мережі; мобільний інтернет.

Savka M.

INTEGRATED DATA COLLECTION MODEL IN MOBILE INTERNET OF THINGS NETWORKS

The Internet of things is considered a new stage in the development of the Internet, where data is exchanged between physical objects connected to the network, and each device can independently interact and establish connections with billions of other things.

The basic concepts of the Internet of things are the organization of interaction between different objects in the environment, the transmission of information that they generate, and the provision of stable connections. Given the novelty, key features, and complexity of the IoT system structure, an important research tool at the design stage is the Mobile IoT network. A comprehensive data collection model based on the analysis of IoT and social IoT models and methods is proposed to improve the security of data collection and improve data management in IoT systems. This integrated model can be used in a variety of IoT applications, such as smart cities, smart transportation, smart buildings, and smart industry. It is noted that the cluster approach significantly increases energy efficiency and reduces network complexity. The proposed model improves management, reduces power consumption and latency, and has many advantages over existing data aggregation models in IoT networks. Various data collection protocols were analyzed in terms of latency, power consumption, security, and mobility support, and data routing methods were developed in dynamic IoT networks. Various data aggregation security models are described, such as access control, authentication, intrusion detection, and trust models, which are the basic mechanisms for building secure systems and are necessary elements of the proposed integrated model. The use of fogging techniques to reduce latency, increase throughput, and improve other network parameters is discussed.

Keywords: data collection model; Internet of things; routing; gateway; wireless networks; mobile internet.

Стаття надійшла до редакції 04.02.2025 р.
Прийнято до друку 11.06.2025 р.