УДК 004.9 **doi: 10.26906/SUNZ.2024.2.078**

Д. О. Дяченко, В. В. Кайда, А. О. Левченко, О. П. Міхаль

Харківський національний технічний університет радіоелектроніки, Харків, Україна

МЕТОДИ ФУНКЦІОНУВАННЯ ПРИСТРОЇВ ІОТ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

Анотація. Актуальність. Функціонування пристроїв Інтернету речей (IoT) з використанням методів машинного навчання (МН) відкриває безліч нових можливостей та переваг. Ці технології дозволяють розширити функціональні можливості традиційних пристроїв, надаючи їм здатність до самонавчання та адаптації до змінюваних умов середовища або поведінки користувачів. IoT пристрої збирають величезні обсяги даних з різних джерел, таких як датчики температури, вологості, руху тощо. МН дозволяє аналізувати ці дані, визначаючи закономірності та тенденції. Використовуючи історичні дані, алгоритми МН можуть передбачати майбутні стани системи або поведінку користувачів, дозволяючи оптимізувати роботу пристроїв. Застосування МН дозволяє IoT пристроям самостійно управляти своїми функціями, наприклад, регулювати освітлення або температуру в будинку, виходячи зі звичок користувачів. Алгоритми можуть аналізувати споживання електроенергії або води і оптимізувати їх використання, зменшуючи витрати та вплив на навколишнє середовище. МН також може допомогти виявити незвичну поведінку або спроби несанкціонованого доступу до системи, підвищуючи рівень безпеки. Здатність до анонімізації та захисту даних, що обробляються IoT пристроями, є критичною, особливо в контексті зростаючих занепокоєнь щодо приватності. Таким чином, використання МН в IoT розкриває потенціал для створення інноваційних рішень, які роблять наше життя зручнішим, безпечнішим та ефективнішим, що і робить тему досліджень в цій області актуальною. **Метою даної роботи** є аналіз методів функціонування пристроїв IoT. **Об'єктом дослідження** є методи збору, обробки та передачі даних в обчислювальних вузлах IoT. **Предметом дослідження** є керування обчислювальними вузлами IoT за допомогою машинного навчання. **Результати.** Проведено аналіз методів функціонування пристроїв IoT. Застосування методів зменшення затримки передачі сигналів вимагає врахування специфіки конкретної IoT системи, включаючи вимоги до затримки, типи даних, обчислювальні та мережеві ресурси, а також потреби користувачів або процесів, які вона обслуговує. При використанні методів зниження обсягу даних, що передаються, слід брати до уваги те, що вони вимагають ретельного планування та налаштування системи IoT, враховуючи специфіку застосування, типи даних та комунікаційні мережі. Це допоможе забезпечити оптимальне використання ресурсів, підвищення масштабованості та зниження вартості експлуатації IoT систем. Впровадження методів конфеденційності та безпеки даних вимагає комплексного підходу до безпеки на всіх етапах життєвого циклу IoT системи, від розробки та виробництва до експлуатації та зняття з експлуатації пристроїв. Основними викликами у зборі та аналізі даних в IoT є забезпечення безпеки та конфіденційності даних, обробка великих обсягів даних в реальному часі, а також потреба в ефективних методах МН, здатних адаптуватися до динамічних умов і змінних середовищ. Інтеграція передових технологій МН в IoT відкриває широкі можливості для створення більш інтелектуальних, ефективних та автономних систем, які можуть революціонізувати багато сфер життя, від розумних будинків до індустріального Інтернету речей.

Ключові слова: машинне навчання, обчислювальний вузол, IoT, датчик, протокол, FPGA.

Вступ

Збір даних є першим кроком, при якому IoT пристрої використовують вбудовані датчики або зовнішні інтерфейси для збору інформації про навколишнє середовище або про специфічні події [1]. Ці дані можуть включати різноманітні параметри, такі як температура, вологість, тиск, рівень освітленості, звук, вібрації, а також більш складні дані, такі як зображення або відео, зібрані з камер. Зібрані дані передаються до центральної системи або хмари для подальшого аналізу. Це може бути зроблено через різні бездротові або провідні комунікаційні технології, такі як Wi-Fi, Bluetooth, ZigBee, LTE, або через спеціалізовані IoT протоколи, наприклад, MQTT або CoAP. На цьому етапі використовуються алгоритми машинного навчання та аналітики даних для обробки та аналізу зібраних даних. Це дозволяє виявляти закономірності та тенденції в даних, робити прогнози на основі історичних даних, розпізнавати аномальні або небажані стани.

Для завдань обробки та класифікації даних можуть використовуватися методи машинного навчання, які обираються з оглядом на залежність від конкретних задач та доступних даних.

На основі аналізу та висновків, отриманих із даних, IoT пристрої можуть автоматично або за вказівкою користувача виконувати певні дії. Наприклад, регулювання температури в приміщенні, оповіщення про потенційні проблеми або автоматичне вимкнення пристроїв у разі виявлення аномалій.

Обробка даних безпосередньо в вузлах IoT стає все більш популярною, оскільки це дозволяє зменшити затримку в обробці даних, знизити обсяг переданих даних і підвищити ефективність загальної роботи системи IoT. Цей підхід, відомий також як обчислення edge computing [2], передбачає виконання аналітичних алгоритмів та обробку даних безпосередньо на крайніх вузлах мережі, де збираються дані, замість того, щоб передавати їх до центральної оброблювальної системи або хмари. Обробка даних безпосередньо на пристрої дозволяє швидше реагувати на зміни в даних, що є критично важливим для додатків, чутливих до затримки, таких як системи автоматичного керування або безпеки. Відсіювання, агрегація та попередня обробка даних на крайніх вузлах знижують необхідність передавати великі обсяги даних через мережу, що може знизити витрати на передачу даних і навантаження на мережеву інфраструктуру. Обробка чутливих або особистих даних

 © Дяченко Д. О., Кайда В. В., Левченко А. О., Міхаль О. П., 2024

безпосередньо на пристрої може допомогти забезпечити їхню конфіденційність, мінімізуючи ризики, пов'язані з передачею даних через вразливі мережі.

Для обробки даних на крайніх вузлах використовуються легковісні версії алгоритмів МН, оптимізовані для роботи на обмежених за ресурсами пристроях. Це можуть бути, наприклад, спрощені моделі нейронних мереж, алгоритми розпізнавання образів або часових рядів. Існує низка розробок і платформ, які полегшують розробку та розгортання додатків для обчислень на краю мережі, такі як AWS Greengrass, Azure IoT Edge та Google Cloud IoT Edge [3]. Обчислювальні можливості та обсяг пам'яті крайніх вузлів часто обмежені, що вимагає оптимізації алгоритмів та програмного забезпечення для ефективної роботи в таких умовах.

Управління розподіленими вузлами та їх масштабування можуть бути складними, особливо в великих масштабованих системах IoT. Розвиток технологій та інструментів для обчислень на краю мережі продовжує спрощувати інтеграцію і розширення можливостей IoT систем, дозволяючи створювати все більш інтелектуальні та автономні рішення.

Отже**, метою цієї роботи** є аналіз методів функціонування пристроїв IoT.

Основна частина

Зменшення затримки в системах IoT є критично важливим для багатьох застосунків, особливо тих, що вимагають швидкого реагування в реальному часі, таких як моніторинг критичних систем, автоматизоване виробництво та інтелектуальні транспортні системи. Переміщення обробки даних з центральних хмарних серверів на крайні вузли, ближче до джерела даних, дозволяє зменшити час передачі даних і затримку в обробці. Це допомагає забезпечити швидке реагування на події в реальному часі. Використання розподілених архітектур, де обробка даних відбувається на багатьох вузлах одночасно, допомагає зменшити затримку, розподіляючи навантаження і знижуючи час очікування обробки на одному сервері. Використання ефективних мережевих протоколів, оптимізованих для IoT, таких як Message Queuing Telemetry Transport (MQTT) або Constrained Application Protocol (CoAP), які розроблені для забезпечення низької затримки і високої ефективності в мережах з обмеженими ресурсами [4]. Мінімізація обсягу обробки даних, необхідної для виконання конкретного завдання, шляхом використання більш ефективних алгоритмів і видалення зайвих обчислювальних процесів може значно знизити затримку. Встановлення пріоритетів для різних типів даних і трафіку може забезпечити, що критично важливі дані обробляються та передаються з найменшою затримкою. Агрегація та попередня обробка даних безпосередньо на IoT вузлах перед їхньою передачею може знизити обсяг переданих даних і, відповідно, зменшити затримку, пов'язану з їх передачею. Також можливе застосування спеціалізованого обладнання, такого як FPGA (польові програмовані вентильні матриці) або GPU (графічні процесорні одиниці), для прискорення обчислень може значно знизити затримку обробки даних. FPGA можуть бути програмовані для виконання специфічних завдань обробки сигналів або даних, що робить їх ідеальними для застосувань, де потрібна висока швидкість обробки і мінімальна затримка в області IoT. FPGA можуть бути перепрограмовані на місці, щоб виконувати різні завдання або адаптуватися до змін у проектних вимогах. Завдяки паралельній обробці даних FPGA можуть обробляти великі обсяги даних з мінімальними затримками, що є критично важливим для деяких IoT-застосувань. FPGA можуть бути оптимізовані для мінімізації споживання енергії, що є важливим для пристроїв IoT, які часто працюють від батарей. Інтеграція FPGA та МН в IoT дозволяє створювати високоефективні, адаптивні та інтелектуальні системи. FPGA можуть бути використані для швидкої обробки даних від сенсорів IoT та виконання алгоритмів МН в реальному часі [5], тоді як МН може надати засоби для аналізу цих даних, прийняття рішень та прогнозування.

Ця інтеграція відкриває широкі можливості для розробки інноваційних IoT-рішень у таких галузях, як розумні будинки, промисловий інтернет речей (IIoT) [6], розумні міста, охорона здоров'я та багато інших.

Слід також відзначити адаптивне керування мережею, яке включає в себе автоматичне регулювання маршрутизації трафіку та керування пропускною спроможністю в залежності від поточного навантаження. Це може допомогти оптимізувати затримку в динамічно змінюваних мережевих умовах.

Зниження обсягу переданих даних у вузлах IoT є важливим аспектом оптимізації IoT систем, що дозволяє підвищити ефективність використання мережі, знизити витрати на передачу даних, зменшити енергоспоживання і покращити масштабованість системи. Перед тим як передавати дані на сервер або в хмару, можливо виконати попередню обробку даних безпосередньо на вузлі. Це включає агрегацію (наприклад, обчислення середніх значень з декількох вимірювань), фільтрацію неважливих даних, компресію та інші форми обробки для зменшення обсягу даних, які потрібно передати. Використання алгоритмів компресії даних дозволяє зменшити їх обсяг перед передачею. Існують різні техніки компресії, від простого кодування до більш складних алгоритмів, що призначені для конкретних типів даних (наприклад, зображень, аудіо або тексту). Замість постійної передачі всіх зібраних даних, вузли можуть передавати дані лише при виявленні значущих змін або подій. Це дозволяє знизити кількість переданих даних, відправляючи інформацію лише тоді, коли це дійсно необхідно.

Використання легковісних протоколів передачі даних, як-от MQTT або CoAP, які мають менший розмір заголовків порівняно з HTTP, може знизити загальний обсяг переданих даних. Передача лише змін у даних замість повного набору даних може значно знизити обсяг передачі. Це особливо ефективно для додатків, де дані змінюються повільно або де можливо передавати лише різницю від попереднього стану. Регулювання частоти, з якою вузли

відправляють дані, на основі поточних умов або важливості інформації, може допомогти знизити обсяг переданих даних. Наприклад, в періоди низької активності чи стабільності системи можна зменшити частоту відправлення.

Сучасні датчики та вузли часто оснащені вбудованими можливостями для попередньої обробки даних. Вибір таких інтелектуальних компонентів може допомогти мінімізувати обсяг переданих даних завдяки вищій ефективності локальної обробки.

Наступним питанням є підвищення конфіденційності та безпеки в вузлах IoT, що є одним з ключових аспектів при розробці та експлуатації IoT систем. Оскільки IoT пристрої часто збирають, обробляють та передають чутливі дані, важливо забезпечити їх належний захист. Можливе використання стандартів шифрування, таких як Transport Layer Security (TLS), для захисту даних під час їх передачі між IoT вузлами та серверами або хмарою або ж застосування сильного шифрування для зберігання даних на пристроях, щоб запобігти їх витоку у разі фізичного доступу до пристрою. Потрібно управління доступом за рахунок реалізації багатофакторної аутентифікації для доступу до системи управління IoT та/або використання сертифікатів та управління ключами для аутентифікації IoT вузлів і забезпечення взаємної аутентифікації між пристроями.

Ще одним фактором, який впливає на конфедіційність є мінімізація даних, тобто актуальними є збір та зберігання лише тих даних, які необхідні для роботи IoT системи, що допоможе зменшити ризики, пов'язані з їх можливим витоком та регулярне видалення зайвих або застарілих даних з пристроїв. Не буде зайвим і автоматичне або полегшене ручне оновлення програмного забезпечення та патчів безпеки для IoT пристроїв, що є критично важливим для захисту від відомих уразливостей. Використання безпечних механізмів оновлення, які перевіряють автентичність та цілісність оновлень перед їх встановленням.

Іншими факторами є захист вузлів IoT від несанкціонованого фізичного доступу, особливо в місцях з високим ризиком такого доступу; розробка та реалізація стратегій для виявлення безпекових інцидентів та аномалій у роботі IoT систем; розділення IoT пристроїв від інших частин мережі за допомогою віртуальних приватних мереж або мережевих вогнів для зниження ризику поширення вразливостей та Проведення регулярних безпекових аудитів та тестувань на проникнення для виявлення потенційних вразливостей у IoT системах.

Для більшості проаналізованих методів та факторів функціонування вузлів IoT можливе застосування МН. МН відіграє ключову роль у розвитку та функціонуванні вузлів IoT, надаючи пристроям здатність до самонавчання, адаптації та автономного прийняття рішень без безпосереднього людського втручання. Інтеграція МН дозволяє IoT системам бути більш інтелектуальними, ефективними та надійними. Воно також дозволяє вузлам IoT обробляти великі обсяги даних локально, визначаючи значущу інформацію або виявляючи аномалії без необхідності передачі всіх даних на центральний сервер або в хмару. Це може значно зменшити затримку в обробці даних та енергоспоживання пристрою.

Алгоритми МН можуть аналізувати історичні дані та на основі них робити прогнози щодо майбутнього стану системи або поведінки користувачів. Це дозволяє IoT системам адаптуватися до змінних умов або потреб, наприклад, автоматично регулювати температуру у розумному будинку або оптимізувати енергоспоживання в індустріальних процесах.

Також МН може допомогти оптимізувати роботу IoT пристроїв, забезпечуючи максимальну ефективність при мінімальному споживанні енергії. Алгоритми можуть аналізувати режими роботи пристроїв та адаптувати їх для зменшення енергоспоживання, наприклад, шляхом управління режимами сну або активності.

Звичайно, що є і деякі обмеження, які пов’язані з використанням МН. Слід відзначити, що IoT вузли часто обмежені в обчислювальних потужностях та енергоспоживанні, що вимагає оптимізації алгоритмів машинного навчання для їх ефективної роботи. Ще одним недоліком є те, що впровадження МН в IoT вимагає додаткових заходів для забезпечення безпеки даних та приватності користувачів. Підтримка та оновлення моделей машинного навчання в розподілених IoT системах може бути складним завданням та вимагати нових підходів в області розробки.

Розгляд концепції IoT дозволяє зробити висновок, що пристрої IoT можуть виступати в ролі обчислювальних вузлів для розподіленої інформаційної системи. В даний час є тенденція на перенесення обробки даних з централізованих систем (хмарні обчислення) на рівень центру обробки даних (туманні обчислення) і далі рівень кінцевих пристроїв (граничні обчислення). Таким чином, з'являється можливість задіяти суттєві обчислювальні потужності, які раніше не використовувалися або використовувалися вкрай обмежено. Розподіл обчислень по безлічі обчислювальних вузлів дозволяє говорити про паралельні обчислення, які в ситуації використання незалежних обчислювальних пристроїв, які є розподіленими системами. Залежно від організації взаємозв'язку між обчислювальними вузлами також говорять про кластерні системи: використання IoT як розподіленої інформаційної системи дозволяє побудувати слабозв'язану кластерну систему [7–9].

Пристрої IoT мають свою специфіку та ряд обмежень, які для організації процесу вирішення обчислювальних завдань не дозволяють використовувати підходи, що використовуються у класичних паралельних та розподілених обчислювальних системах.

Висновки

У даній роботі проведено аналіз методів функціонування пристроїв IoT. Застосування методів зменшення затримки передачі сигналів вимагає врахування специфіки конкретної IoT системи, включаючи вимоги до затримки, типи даних, обчислювальні та мережеві ресурси, а також потреби користувачів або процесів, які вона обслуговує.

При використанні методів зниження обсягу даних, що передаються, слід брати до уваги те, що вони

вимагають ретельного планування та налаштування системи IoT, враховуючи специфіку застосування, типи даних та комунікаційні мережі. Це допоможе забезпечити оптимальне використання ресурсів, підвищення масшта-бованості та зниження вартості експлуатації IoT систем.

Впровадження методів конфеденційності та безпеки даних вимагає комплексного підходу до безпеки на всіх етапах життєвого циклу IoT системи, від розробки та виробництва до експлуатації та зняття з експлуатації пристроїв.

Таким чином, основними викликами у зборі та аналізі даних в IoT є забезпечення безпеки та конфіденційності даних, обробка великих обсягів даних в реальному часі, а також потреба в ефективних методах машинного навчання, здатних адаптуватися до динамічних умов і змінних середовищ. Інтеграція передових технологій машинного навчання в IoT відкриває широкі можливості для створення більш інтелектуальних, ефективних та автономних систем, які можуть революціонізувати багато сфер життя, від розумних домів до індустріального Інтернету речей.

СПИСОК ЛІТЕРАТУРИ

1. Дяченко В. Інтелектуальні підходи енергозбереження у безпровідних сенсорних комп'ютерних мережах // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2020. – Т. 4 (62). – С. 114-118. – doi:https://doi.org/10.26906/SUNZ.2020.4.114.
2. Anand B., Edwin A., Hao J. Gamelets – Multiplayer mobile games with distributed micro-clouds". Seventh International Conference on Mobile Computing and Ubiquitous Networking (ICMU). 2014. pp. 14–20. doi:10.1109/ICMU.2014.6799051.
3. Verma A., Pedrosa L., Korupolu M., Oppenheimer D.; Tune E., Wilkes J. Large-scale cluster management at Google with Borg". Proceedings of the Tenth European Conference on Computer Systems. Article 18, sec. 2.1 (p. 1), sec. 6.1 (p. 11).2015. doi:10.1145/2741948.2741964
4. Boyd B., Gauci J., Robertson M., Nguyen V., Gupta R., Gucer V., Kislicins V. Building Real-time Mobile Solutions withMQTT and IBM MessageSight. IBM.2014.p.21-38.
5. Xing Y. et al. MPTCP Meets Big Data: Customizing Transmis-sion Strategy for Various Data Flows //IEEE Network. – 2020. – Т. 34. – №. 4. – С. 35-41.
6. Khan I., Chen K. EBA: Efficient Bandwidth Aggregation for Connected Vehicles with MPTCP //IEEE Internet of Things Journal. – 2021.
7. Коваленко А. А., Кучук Г. А. Методи синтезу інформаційної та технічної структур системи управління об'єктом критичного застосування. *Сучасні інформаційні системи*. 2018. Т. 2, № 1. С. 22–27. DOI: https://doi.org/10.20998/2522-9052.2018.1.04
8. Свиридов А. С., Коваленко А. А., Кучук Г. А. Метод перерозподілу пропускної здатності критичної ділянки мережі на основі удосконалення ON/OFF-моделі трафіку. *Сучасні інформаційні системи*. 2018. Т. 2, № 2. С. 139–144. DOI: https://doi.org/10.20998/2522-9052.2018.2.24
9. Palash M. R., Chen K., Khan I. Bandwidth-need driven energy efficiency improvement of MPTCP users in wireless networks //IEEE Transactions on Green Communications and Networking. – 2019. – Т. 3. – №. 2. – С. 343-355.

Received (Надійшла) 26.01.2024
Accepted for publication (Прийнята до друку) 27.03.2024

Operation methods of IoT devices using machine learning

Dmytro Dyachenko, Valeriya Kaida, Anton Levchenko, Oleg Mikhal

Abstract. Relevance. The functioning of Internet of Things (IoT) devices using machine learning (ML) methods opens up many new op-portunities and advantages. These technologies make it possible to expand the functionality of traditional devices, giving them the ability to self-learn and adapt to changing environmental conditions or user behavior. IoT devices collect huge amounts of data from various sources such as temperature, humidity, motion sensors, etc. MN allows you to analyze these data, identifying patterns and trends. Using historical data, machine learning algorithms can predict future system states or user behavior, allowing devices to be optimized. The application of MN allows IoT devices to independently manage their functions, for example, to regulate lighting or temperature in the house, based on your habits and preferences. Algorithms can analyze electricity or water consumption and optimize their use, reducing costs and impact on the environment. MH can also help detect unusual behavior or attempts to gain unauthorized access to the system, increasing security. The ability to anonymize and protect data processed by IoT devices is critical, especially in the context of growing privacy concerns. Thus, the use of MH in IoT reveals the po-tential for creating innovative solutions that make our lives more convenient, safer and more efficient, which makes the topic of research in this area relevant. **The purpose** is to analyze the methods of functioning of IoT devices. **The object** is methods of data collection, pro-cessing and transmission in IoT computing nodes. **The subject** is the control of IoT computing nodes using machine learning. **Results**. An analysis of the methods of functioning of IoT devices was carried out. Applying methods to reduce signal transmission delay requires consideration of the specifics of a particular IoT system, including latency requirements, data types, computing and network resources, and the needs of the users or processes it serves. When using methods to reduce the amount of data transmitted, it should be taken into account that they require careful planning and configuration of the IoT system, taking into account the specifics of the application, data types and communication networks. This will help ensure optimal use of resources, increase scalability and reduce the cost of operating IoT systems. The implementation of data privacy and security methods requires a comprehensive approach to se-curity at all stages of the IoT system life cycle, from development and production to operation and decommission-ing of devices. The main challenges in data collection and analysis in IoT are ensuring data security and privacy, processing large volumes of data in real time, as well as the need for effective machine learning methods that can adapt to dynamic conditions and changing environments. The integration of advanced machine learning technolo-gies into the IoT opens up vast opportunities for creating more intelligent, efficient and autonomous systems that can revolutionize many areas of life, from smart homes to the industrial Internet of Things.

Keywords: machine learning, computing node, IoT, sensor, protocol, FPGA.