МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧОРНОМОРСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ПЕТРА МОГИЛИ

Лаптін Іван Максимович

УДК 004.75

Програмна система для взаємодії з пристроями Internet-of-Things на базі протоколу CoAP

Напрям підготовки 6.050102 – Комп’ютерна інженерія

Автореферат
бакалаврської роботи
на здобуття кваліфікації бакалавра з комп’ютерної інженерії

Миколаїв – 2019

Робота виконана у Чорноморському національному університеті ім. Петра Могили.

Керівник: канд. тех. наук
Ярослав Михайлович Крайник,
ЧНУ ім. Петра Могили,
ст. викладач

Рецензент: д-р педагогічних наук, професор
Мещанінов Олександр Павлович**,**
ЧНУ ім. Петра Могили
викладач

Консультант: д-р біол. наук, професор
Людмила Іванівна Григор'єва**,**
ЧНУ ім. Петра Могили,
завідувач кафедри екології Медичного інституту

Захист відбудеться « 26 » червня 2019 р. о 10^{00} на засіданні Державної екзаменаційної комісії в ЧНУ ім. Петра Могили, ауд. 2-406

З бакалаврською роботою можна ознайомитись на сайті ЧНУ ім. Петра Могили за посиланням http://chmnu.edu.ua

Автореферат оприлюднений « 18 » червня 2019 р.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Одним з широко використовуваних протоколів для взаємодії між IoT-пристроями (Internet of Things) і зовнішнім середовищем є протокол CoAP - Constrained Application Protocol. Протокол CoAP призначений для взаємодії простих пристроїв, наприклад датчиків малої потужності, вимикачів, клапанів, які управляються або контролюються віддалено через мережу Інтернет. Такі пристрої використовуються в області Інтернету речей, а породжуваний ними інформаційний обмін називається міжмашинною взаємодією (M2M). Часто подібні пристрої називають пристроями з обмеженими ресурсами. Вони зазвичай мають обмежений енергоресурс, невеликий обсяг пам'яті і невисоку потужність, тому в роботі з ними важливо забезпечувати низькі енерговитрати, використовувати передачу повідомлень малого обсягу. Протокол CoAP забезпечує взаємодію цих пристроїв, щоб виконувати всі необхідні вимоги. Мережа, в якій працюють такі пристрої, називають мережею з обмеженими ресурсами.

Істотна особливість протоколу CoAP - це його сумісність з протоколом HTTP, що забезпечує при його використанні взаємодію сукупності пристроїв IoT, які формують якусь мережу, з всесвітньою павутиною Інтернету.

Мета: розробка системи збору даних с датчиків що використовують протокол CoAP.

Для досягнення мети в бакалаврській роботі поставлені та вирішені наступні **задачі**:

- проаналізування відомих систем збору даних;
- вибрати протокол для збору даних;
- вибрати апаратну платформу для реалізації та тестування системи;
- розробити серверну та клієнтську частину для збору даних з вузлів мережі за допомогою протоколу CoAP;
- розглянути питання з охорони праці та безпеки життєдіяльності.

Об’єкт: Технології бездротових сенсорних мереж.

Предмет: Програмно-апаратний компекс збору данних.

Використані методи: методи та засоби комп'ютерних мереж, методи взаємодії між елементами комп'ютерних мереж, клієнт-серверні технології, технології програмування відповідно до шаблонів програмування, методи бездротової передачі даних.

Практичне значення одержаних результатів: ESP8266 може працювати як в ролі точки доступу WiFi так і кінцевої станції.

Структура та обсяг роботи. Бакалаврська робота складається з анотації на 2 сторінках, вступу, трьох розділів, висновків, переліку джерел посилання з 15 найменувань, 1 додаток на 12 сторінках. Основна частина роботи становить 69 сторінок, серед яких 9 рис. та 1 табл.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** подано обґрунтування актуальності теми бакалаврської роботи, зазначено її зв’язок із науковою програмою, планами і темами, сформульовано мету та завдання дослідження, вказано практичне значення одержаних результатів, наведено відомості про апробацію результатів роботи та публікації автора. Задача отримання даних з датчиків і аналізування їх.

У **першому розділі** бакалаврської роботи «Аналітичний огляд» розлянуто основні теми пов’язані з Кібер-фізичними системами,Інтернет речами, а також проблеми інтернет речей.

Гідність IoT пристроїв у тому, що більшість цих пристроїв дуже прості. Наприклад, ви можете підключити до вашої домашньої Wi-Fi мережі кава-машину. Проте за все доводиться платити. Найбільша проблема полягає в тому, що більшість виробників IoT пристроїв не мають досвіду забезпечення безпеки побутової техніки, яку виробляють. Деякі виробники – новачки на ринку; їх мета – швидко і з найменшими витратами розробити новинку і вивести її на ринок, наприклад через Kickstarter. Ці компанії зосереджені на прибутку, а не на

безпеці. Результатом цього є те, що більшість пристроїв IoT мають дуже слабкий захист або його немає зовсім. У деяких пристроях встановлені стандартні паролі, які можна знайти в Інтернеті, і їх не можна змінити. Крім того, в більшості IoT пристроїв навіть немає можливості їх налаштувати, ви можете використовувати тільки стандартну заводську конфігурацію. Багато з цих пристроїв дуже складно або неможливо оновити. В результаті, ці пристрої дуже швидко застарівають, їх вразливості стають добре відомими, і немає можливості їх усунути. Все це робить вас уразливими.

На даному етапі розвитку технологій і суспільства Інтернет речей активно впроваджується не в глобальних масштабах, а всередині компаній, що займаються виробництвом товарів, енергії, транспортними перевезеннями і т.п. - там, де за рахунок нових технологій очікується підвищення продуктивності та конкурентоспроможності. Складність масштабування цього досвіду обумовлена тим, що необхідно інтегрувати в єдине ціле багато систем від різних постачальників, а налагодити їх злагоджену роботу - завдання складніше, ніж домогтися гармонійного звучання Великого симфонічного оркестру.

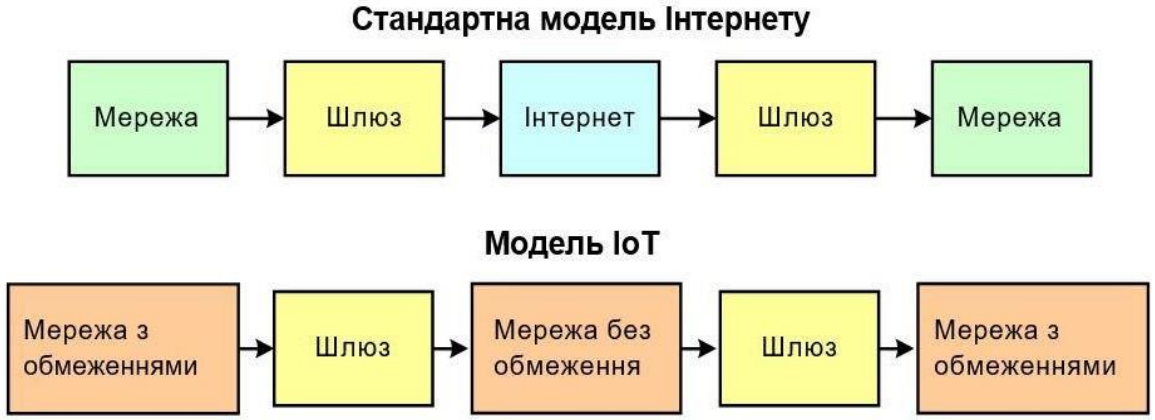

Рисунок 1 – Порівняння моделей передачі даних в Інтернеті і в IoT

У **другому розділі** бакалаврської роботи «Розробка аппаратної частини» проведено аналіз відомих систем збору даних,перечісленні классификациі датчиков та вибір апаратної платформи для реалізації. Arduino — апаратна платформа для розробки електронних пристроїв, основними компонентами якої є мікроконтролер (МК) з портами вводу/виводу та середовище розробки

ArduinoIDE. Програмування контролера здійснюється на мові Wiring, що є підмножиною C/C++. Усе сімейство контролерів Arduino, окрім версій «Mini» і «ProMini», мають інтегрований на плату перетворювач інтерфейсів USB-UART (USB-TTL), який дозволяє програмувати мікроконтролер без зовнішнього програматора. Дана особливість реалізується також використанням раніше записаної у МК програми-завантажувача (Bootloader). В актуальних насьогодні версіях Arduino використовується контролер ATmega328 компанії Atmel для плат версій Uno, Nano, ProMini з 32 кБайт пам'яті. У платі Mega2560 використовується МК ATmega2560 з 256 кБайт пам'яті.

Платформа Інтернету речей має бути здатна обслуговувати величезну кількість даних, а тому бути високоефективною. Відмітимо деякі аспекти, які дозволяють цього досягти.

По-перше, величезний вплив на продуктивність має організація мережевого вводу/виводу. Описана проблема 10000 з'єднань – задача оптимізації коду та конфігурації сервера так, аби мати можливість обслуговувати паралельно велику кількість з'єднань.

Традиційний метод, який був популярним деякий час тому, передбачав використання одного потоку операційної системи на з'єднання. Наприклад, якщо надходить запит на зчитування даних із бази, потік надсилає його та блокується до того моменту, як від СКБД надійде відповідь. При надходженні іншого запиту до сервера він запускає новий потік.

Насправді важко переоцінити, наскільки приголомшливо виглядають і працюють плати на основі ESP8266, такі як Wemos D1 Mini. За буквально пару доларів ви можете отримати в зручному форм-факторі пристойно потужний мікроконтролер з підтримкою Wi-Fi, який має достатню кількість цифрових контактів для виконання корисних завдань Інтернету речей. Як і Arduino і Raspberry Pi, ESP8266 - це пристрій, який відкриває всі нові області розробки електроніки, які просто не були такими практичними або економічними, як раніше.

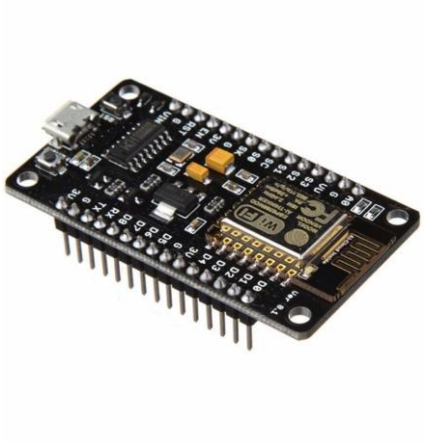

Рисунок 2 – Модуль ESP8266

Мікроконтролер ESP8266 - мініатюрний WiFi модуль на базі новітньої мікросхеми ESP8266 з вбудованим стеком протоколу TCP/IP і управлінням AT-командами. Чіп створений для використання в розумних розетках, mesh-мережах, IP-камерах, бездротових сенсорах, носимій електроніці і т.д. Призначення ESP8266 стати мозком майбутнього «Інтернету речей».

Передбачено два варіанти використання чіпа: 1) у вигляді моста UART-WIFI, коли модуль на базі ESP8266 підключається до існуючого рішення на базі будь-якого іншого мікроконтролера і управляється AT-командами, забезпечуючи зв'язок рішення з інфраструктурою Wi-Fi; 2) реалізуючи нове рішення, яке використовує сам чіп ESP8266 в якості керуючого мікроконтролера.

Компанія Espressif Systems постійно здійснює науково-дослідних і проектну діяльність в області Wi-Fi і Bluetoothтехнологій. В результаті чого, продукція Espressif широко відома в усьому світі і використовується в мобільних пристроях, побутової техніки та промислових додатках.

У **третьому розділі** бакалаврської роботи «Розробка програмної частини» описані методи для взаемодіі кліенту с сервером на базі протоколу CoAP,основні характеристики протоколу,методи защіти, кешування та приклади программи. Протокол обмежених додатків (CoAP) являє собою протокол веб-передачі RESTful для обмежених в ресурсах мереж і вузлів. CoAP.NET - це реалізація в C #, що надає послуги на основі CoAP додатків .NET.

Відгуки і пропозиції будуть оцінені. Сеанси CoAP розглядаються як пара запит-відповідь.

Сервери CoAP зазвичай відповідають на пакет запиту відповідним пакетом. Цей відповідь пакет може бути значно більше, ніж пакет запиту. Зловмисник може використовувати вузли CoAP, щоб перетворити невеликий пакет атаки в великий пакет атаки, такий підхід називається посиленням. Таким чином, існує небезпека того, що вузли CoAP можуть стати причетними до атак типу «відмова в обслуговуванні» (DoS), використовуючи які посилюють властивості протоколу: зловмисник, який намагається перевантажити жертву, але обмежений в обсязі трафіку, який він може генерувати, може використовуйте посилення , щоб генерувати більший обсяг трафіку.

Це, зокрема, проблема в вузлах, які забезпечують доступ NoSec і які доступні від зловмисника і можуть отримати доступ до потенційних жертв (наприклад, в звичайному Інтернеті), оскільки протокол UDP не дозволяє перевірити адресу джерела, вказаний в пакеті запиту. Зловмиснику потрібно тільки помістити IP-адреса жертви в вихідний адресу відповідного пакета запиту, щоб згенерувати більший пакет, спрямований на жертву.

В якості пом'якшувального фактору обмежені мережі зможуть генерувати тільки невеликий обсяг трафіку, що може зробити вузли CoAP менш привабливими для цієї атаки. Однак, обмежена ємність мережі робить саму мережу імовірною жертвою атаки.

Сервер CoAP може зменшити ступінь посилення, яку він надає зловмисникові, використовуючи режими нарізки / блокування CoAP і пропонуючи великі уявлення ресурсів тільки у відносно невеликих зрізах. Наприклад, для 1000-байтового ресурсу 10-байтовий запит може привести до 80-байтовому відповіді (з 64-байтовим блоком) замість 1016-байтового відповіді, що значно зменшує забезпечується посилення.

CoAP також підтримує використання багатоадресних IP-адрес в запитах, що є важливою вимогою для M2M. Багатоадресні запити CoAP можуть бути

джерелом випадкових або навмисних атак типу «відмова в обслуговуванні», особливо в мережах з обмеженим доступом. Ця специфікація намагається зменшити ефекти посилення багатоадресних запитів шляхом обмеження, коли повертається відповідь. Щоб обмежити можливість коректного використання, сервери CoAP не повинні приймати багатоадресні запити, які не можуть бути автентифіковано. Якщо можливо, сервер CoAP повинен обмежити підтримку багатоадресних запитів конкретними ресурсами, де потрібна ця функція.

У деяких операційних системах загального призначення, що надають API в стилі Posix, непросто з'ясувати, чи був отриманий пакет адресований за адресою під LGPL. Хоча багато реалізації знатимуть, приєдналися вони до многоадресной групі, це створює проблему для пакетів, адресованих багатоадресних адресами в формі FF0x :: 1, які приймаються кожним вузлом IPv6. Реалізації повинні використовувати сучасні API.

Дотримуючись стандартів і відкритих специфікацій, можна поліпшити сумісність розробки в сфері IoT з існуючими системами. Аналогічно, використовуючи відкриті, стандартизовані, взаємозамінні компоненти, можна уникнути необхідності створення дорогої інфраструктури. А правильний вибір шаблону обміну даними - це відмінний спосіб убезпечити себе від серйозної переробки проекту на пізніх стадіях його розвитку.

Додатки містять лістинг коду обробки даних на сервері.

У спеціальній частині «Охорона праці при роботі з програмним забезпеченням пов’язаним з приняттям рішень» наведено аналіз факторів виробничого середовища під час експлуатації електронно-обчислювальних машин, а також визначений вплив цих факторів на здоров’я та працездатність працівників. Слід зазначити, що було встановлено відповідність всіх розглянутих показників чинним санітарним нормам та виявлено

ВИСНОВКИ

У дипломній роботі розглянуті найбільш популярний протокол Інтернету Речей CoAP, який використовується для відправки інформації від датчика до сервера. В ході дослідження виявлено, що для протокол CoAP характерний менш накладні витрати на передачу даних (у зв'язку з невеликою кількістю службового трафіку) і меншою смуги пропускання, ніж чим у протоколу HTTP / 2. Дані протоколи добре адаптовані для маломощних пристроїв Інтернету Речей на базі мікроконтролерів. Для своєї роботи протокол CoAP не вимагає постійного з'єднання між клієнтом і сервером.

Експериментальні результати показали, що ефективність розглянутих протоколів залежить від різних умов мережі зв'язку.

Найбільш оптимальним є протокол CoAP, в якому можливо задавати параметри, що відповідають за надійність доставки повідомлень.. У зв'язку з цим, в даний час правильний вибір протоколів для різних Інтернет Речей допомагає вирішити задачу економії ресурсів як енергоспоживання, так і гарантірованной доставкі. Особливо це актуально у зв'язку зі збільшенням кількості пристроїв Інтернету Речей. Так за даними J'son & Partners Consulting, незважаючи на поточні проблеми в економіці, до 2018 го- ду ринок Інтернету Речей в Україні досягне рівня в 32 млн. Підключених пристроїв.

АНОТАЦІЯ

Лаптін І.М. Програмна система для взаемодії з пристроями Internet-of-Things на базі протоколу CoAP. – Кваліфікаційна робота бакалавра зі спеціальності 6.050102 Комп’ютерна інженерія на здобуття кваліфікації «фахівець з інформаційних технологій». – Чорноморський національний університет імені Петра Могили, 2019.

Бакалаврська робота спрямована на дослідження взаемодії з пристроями Internet-of-Things на базі протоколу CoAP. Розглянуто протокол CoAP, язик програмування C# и мікроконтролер китайського виробника esp8266.

Практичне значення результатів дослідження та розроблення поляга обработці і аналізування даних з мікроконтролерів на сервері.

Пояснювальна записка бакалаврської роботи складається зі вступу, трьох розділів, висновків та одного додатку. У вступі визначається актуальність теми, сформульована мета, об’єкт, предмет та завдання дослідження та розроблення бакалаврської роботи. У першому розділі досліджується аналітичний огляд літератури та патентної інформації; проводиться аналіз його економічних показників та основних методів аналізу. У другому розділі проводиться аналіз відомих систем збору даних що найбільше підходять для обробки данних з мікроконтролера esp8266. У третьому розділі наведені алгоритми передачі даних. У висновках наведено аналіз виконаної роботи та отриманих результатів дослідження та розроблення. У додатку А наведений лістинг основних класів програми.

Також розглянуто питання з охорони праці та безпеки у надзвичайних ситуаціях проаналізовано систему заходів і засобів по запобіганню впливу на людину несприятливих факторів, які супроводжують роботу працівника ІТ-сфери. Виконано аналіз освітлення та мікрокліматичних умов на робочому місці, управління цивільним захистом на підприємстві у разі виникнення пожежі.

Бакалаврська робота містить 69 с. (без додатків), 12 рис.,1 табл., 15 джерел посилання та 1 додатків.

Ключові слова: Інтернет речей, протокол, CoAP, M2M, пристрої, мережу, HTTP, многоадресная розсилка.

ABSTRACT

Laptin I. Automated system for thermal losses reconnaissance in engineering communications based on heatmap research. – Bachelor’s thesis in specialty 6.050102 Computer Engineering. – Petro Mohyla Black Sea National University, 2019.

The Bachelor’s Thesis is devoted forecasting of coordination with CoAP based Internet of Things. For the research were used CoAP, programming language C# and microcontroller esp8266.

The practical significance of the research results consists in processing and analysis of data from microcontrollers on the server.

The professional section includes of introduction, three chapters, conclusions and the one application. In the introduction is determined by the relevance of the topic and provides a brief overview of the task, the aim, object, subject, research and design tasks are presented too. In the first section examines analytical review of literature and patent information, an analysis of its economic indicators and basic methods of analysis. In the second chapter review analyzing known system data areas that are most suitable for data processing of microcontrollers esp8266. The third chapter describes algorithmic software. In conclusion analysis of the work carried out and the results obtained. In an addition A is a listing of the main classes of the program.

Also, the issues of occupational on occupational safety and protection in emergency situations the system of measures and means for preventing the impact on the person of the adverse factors that accompany the work of the IT employee was analyzed. Analysis of lighting and microclimatic conditions in the workplace, management of civil protection in the company in the event of a fire was executed.

Thesis contains 69 pages (without appendices), 12 figures, 1 tables, 15 references and 1 appendices.

Key words: Internet of Things, protocol, CoAP, M2M, devices, network, HTTP, multicast.