УДК 004.424

І.Я. Урсол
І.С. Колесник

Апаратно-програмна система контролю безпеки житлового приміщення під час аварійних ситуацій

Вінницький національний технічний університет

Анотація.
У представленій роботі розглянуто принципи побудови розподіленої гібридної системи контролю безпеки житлового приміщення на основі мікроконтролерів ESP32 та ESP8266. Описано архітектуру бездротової сенсорної мережі (WSN), що складається з центрального хабу та віддалених вузлів-сателітів. Запропоновано алгоритм асинхронної міжмашинної взаємодії (M2M) за протоколом MQTT для локалізації аварійних ситуацій (витік газу, затоплення, проникнення, сейсмічна активність). Реалізовано мобільний інтерфейс для дистанційного керування. Проведено тестування відмовостійкості та швидкодії системи.
Ключові слова: інтернет речей, IoT, система безпеки, розумний дім, розподілена мережа, ESP32, ESP8266, MQTT, міжмашинна взаємодія, датчик витоку газу.

Abstract.
In the presented paper, the principles of designing a distributed hybrid residential security control system based on ESP32 and ESP8266 microcontrollers are considered. The architecture of a wireless sensor network (WSN) consisting of a central hub and remote satellite nodes is described. An algorithm for asynchronous machine-to-machine (M2M) interaction using the MQTT protocol for localizing emergency situations (gas leak, flooding, intrusion, seismic activity) is proposed. A mobile interface for remote control was implemented. Tests were conducted to evaluate the system's fault tolerance and performance.
Keywords: internet of things, IoT, security system, smart home, distributed network, ESP32, ESP8266, MQTT, machine-to-machine interaction, gas leak sensor.

Вступ

Сучасні інформаційні технології та концепція «Інтернету речей» (IoT) активно впроваджуються у сферу автоматизації та захисту житла. Більшість існуючих бюджетних систем безпеки є дротовими або локальними, що суттєво обмежує їх масштабованість та ускладнює монтаж у готових інтер'єрах. Крім того, комерційні рішення часто залежать від хмарних серверів, що призводить до затримок у спрацюванні під час перебоїв з інтернет-з'єднанням.

Одним із перспективних напрямів є використання бездротових сенсорних мереж (WSN) та парадигми граничних обчислень (Edge Computing), які дозволяють здійснювати децентралізований збір даних та забезпечувати миттєве автономне реагування на загрози.

Метою роботи є розроблення розподіленої гібридної апаратно-програмної IoT-системи контролю безпеки житлового приміщення та дослідження алгоритмів підвищення надійності передачі тривожних сигналів у режимі реального часу.

Основна частина

Розроблена система складається з центрального керуючого хабу, віддалених бездротових вузлів-сателітів, виконавчого блоку та мобільного додатка користувача. Обмін даними між апаратними компонентами здійснюється бездротовим шляхом за допомогою технології Wi-Fi та протоколу MQTT, що забезпечує роботу системи в межах локальної мережі без необхідності прокладання сигнальних кабелів. Кожне повідомлення від датчиків передається до обчислювального ядра хабу, де виконується його попередня фільтрація та аналіз.

Для визначення стану середовища використано комплекс різнотипних датчиків. Головний хаб (на базі ESP32) дозволяє визначати рівень сейсмічної активності за допомогою модуля MPU-6050

та концентрацію метану в режимі реального часу за допомогою датчика MQ-2. Отримані координати прискорення та значення загазованості безпосередньо обробляються центральним процесором. Віддалені вузли (на базі ESP8266) виконують точковий моніторинг протікання води та цілісності периметра (PIR-сенсор і геркони).

Алгоритм обробки сенсорних даних та прийняття рішень щодо локалізації аварії виконується у декілька етапів, як наведено на рисунку 1.

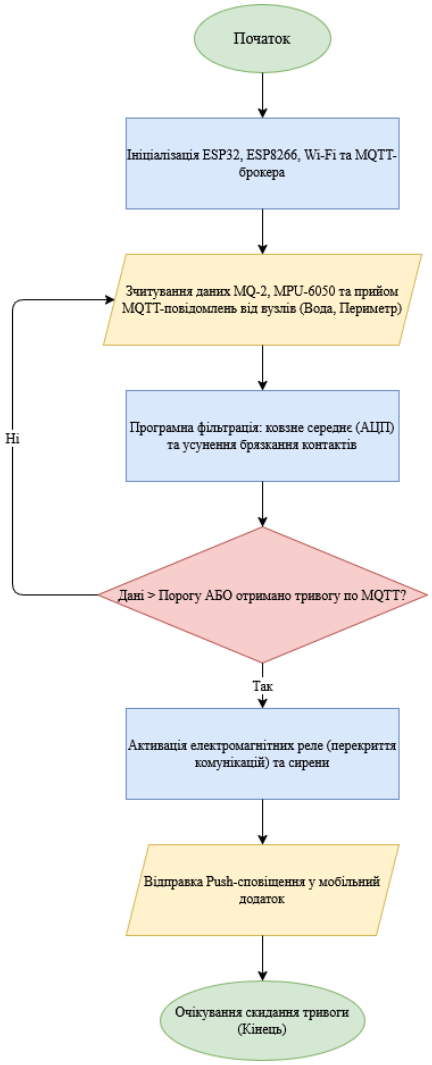

Рисунок 1 – Алгоритм обробки сенсорних даних та M2M-взаємодії у розподіленій системі

На першому етапі визначається стан кожного датчика: система порівнює поточні показники із заданими безпечними порогами. Зокрема, для аналогових датчиків (MQ-2, Water Sensor) вимірюється рівень напруги на АЦП — якщо він перевищує норму, фіксується загроза. Для цифрових датчиків охорони периметра аналізується логічний рівень на GPIO портах, зміна якого генерує апаратне переривання. Для модуля MPU-6050 аналізується зміна прискорення по трьох осях між послідовними циклами вимірювань.

На другому етапі отримана інформація з усіх датчиків агрегується та порівнюється із шаблонами тривожних подій. Наприклад, спрацювання геркона на вхідних дверях відповідає сценарію «Проникнення», а фіксація води вузлом-сателітом — сценарію «Затоплення». Для розпізнавання комплексних загроз центральний хаб об'єднує власні локальні дані з MQTT-повідомленнями від віддалених плат, що дозволяє визначити, який саме виконавчий механізм (реле води чи газу) необхідно активувати.

На третьому етапі виконується стабілізація результатів вимірювань. Оскільки під час роботи аналогових сенсорів та механічних контактів можуть виникати короткочасні помилки (через дрібні побутові випари на кухні, вібрації від закриття дверей або шуми АЦП), тривожна подія

підтверджується лише після програмної фільтрації. Застосовується алгоритм ковзного середнього для згладжування даних MQ-2 та алгоритм усунення брязкання контактів (debouncing) для герконів. Це дозволяє усунути випадкові хибні спрацьовування та підвищити стабільність роботи системи безпеки.

Інтерфейс керування системою реалізовано у вигляді кросплатформного мобільного додатка. Для відображення телеметрії та поточного стану системи використовується підписка на відповідні MQTT-топіки. Інтерфейс забезпечує відображення поточного статусу загроз, кнопок керування електроклапанами, а також можливість дистанційного калібрування датчиків.

Тестування системи проводилось шляхом емуляції базових аварійних ситуацій (витік газу, протікання, вібрації) по 50 повторень кожної в різних умовах розміщення вузлів. Встановлено, що оптимальною є робота сателітів у зоні стабільного покриття домашньої Wi-Fi мережі (до 15–20 метрів від роутера). Аналіз швидкодії показав, що завдяки застосуванню парадигми граничних обчислень (Edge Computing), середній час автономної реакції системи на аварію (від детекції до перекриття комунікацій реле) становить 300–400 мс.

Висновки

Розроблено розподілену апаратно-програмну систему контролю безпеки з використанням мікроконтролерів сімейства ESP та протоколу MQTT. Обґрунтовано вибір дворівневої гібридної архітектури, що дозволило виключити необхідність прокладання сигнальних кабелів та знизити енергоспоживання сенсорної мережі. Запропонований алгоритм M2M-взаємодії та локальної фільтрації даних забезпечує високу швидкість автоматичної локалізації аварій (до 0,4 с), мінімізуючи вплив людського фактора та запобігаючи масштабним матеріальним збиткам.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРЫ

1. Cameron N. Electronics Projects with the ESP8266 and ESP32: Building Web Pages, Applications, and WiFi Enabled Devices. Berkeley: Apress, 2021. 272 p.
2. Соколов А.В. Бездротові сенсорні мережі: архітектура та протоколи. Київ: Наукова думка, 2022. 304 с.
3. MQTT Version 3.1.1 Specification. OASIS Standard. Режим доступу: https://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html
4. ESP32 Series Datasheet. Espressif Systems. Режим доступу: https://www.espressif.com/

Колесник Ірина Сергіївна — кандидат технічних наук, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця, e-mail: iskolesnyk@gmail.com

Урсол Іван Ярославович — студент групи 1СП-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: tualuata@gmail.com

Kolesnyk Iryna Serhiivna — Candidate of Technical Sciences, Associate Professor of the Department of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: iskolesnyk@gmail.com

Ursol Ivan Yaroslavovych — student of group 1SP-22b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: tualuata@gmail.com