

МЕТОД ТА ЗАСОБИ МОНІТОРИНГУ ІОТ-ПРИСТРОЇВ У ЛОКАЛЬНИХ МЕРЕЖАХ ІЗ ВИЯВЛЕННЯМ ВІДМОВ

Вінницький національний технічний університет

Анотація

У роботі розглянуто метод та програмний засіб моніторингу доступності ІоТ-пристроїв у локальних мережах для своєчасного виявлення відмов. Запропонований підхід базується на гібридній L3-діагностиці, що включає періодичну відправку ICMP-запитів для аналізу втрати пакетів (loss) та затримки (latency), а також механізм фіксації відмов з порогом очікування. Розроблено архітектуру рішення у вигляді настільного (desktop) застосунку на Python, що автоматично визначає параметри поточної мережі та дозволяє користувачеві в режимі реального часу відстежувати статус пристроїв, ідентифікувати їх, візуалізувати історію стану на графіках та отримувати оперативні сповіщення у журналі відмов. Це підвищує надійність функціонування "розумної" мережі завдяки комплексній та швидкій діагностиці.

Ключові слова: ІоТ, моніторинг, локальна мережа, виявлення відмов, настільний застосунок, ICMP, Scapy, L3-моніторинг, деградація каналу.

Abstract

The paper considers the method and software tools for monitoring the availability of IoT devices in local networks for timely failure detection. The proposed approach is based on a hybrid L3 diagnostics, which includes periodic ICMP requests to analyze packet loss and latency, as well as a failure detection mechanism with a waiting threshold. A solution architecture has been developed in the form of a desktop application (Python), which automatically detects current network parameters and allows the user to monitor the status of connected devices in real-time, identify them, visualize status history on charts, and receive operational notifications in a failure log. This enhances the operational reliability of the "smart" network due to comprehensive and fast diagnostics.

Keywords: IoT, monitoring, local network, failure detection, desktop application, ICMP, Scapy, L3 monitoring, channel degradation.

Вступ

У сучасних умовах стрімкого розвитку технологій та експоненціального зростання кількості пристроїв, підключених до мережі Інтернет, концепція Інтернету речей (ІоТ) набуває все більшого поширення. ІоТ-системи стали невід'ємною частиною різноманітних сфер... (Текст збігається)... Це зумовлює необхідність розробки простих, локалізованих та доступних засобів, сфокусованих на базових, але критично важливих параметрах — доступності пристрою в мережі.

Актуальним напрямом є створення методу та програмних засобів моніторингу, реалізованих у вигляді настільного (desktop) застосунку, які забезпечують автоматичне виявлення відмов з'єднання пристроїв, підключених до того ж маршрутизатора, і формування оповіщень у режимі реального часу. Розроблення подібного локального та незалежного програмного засобу для моніторингу стану ІоТ-пристроїв є важливим завданням, від ефективного вирішення якого залежить стабільність та керованість сучасної "розумної" інфраструктури.

Результати дослідження

У результаті проведеного дослідження було розроблено прототип настільної системи моніторингу ІоТ-пристроїв у локальній мережі, яка успішно реалізує запропонований метод виявлення L3-відмов. Програмний засіб, розроблений на мові Python з використанням бібліотек Scapy, psutil та CustomTkinter, автоматично визначає параметри поточної мережі (IP-адресу та маску) для ініціалізації сканування, що дозволяє йому працювати в різних мережесередовищах без ручного налаштування.

Метод моніторингу ґрунтується на періодичній відправці ICMP-запитів (ping) до всіх виявлених у мережі пристроїв. Це дозволяє класифікувати стан кожного пристрою на основі двох ключових показників: відсотка втрати пакетів та середньої затримки (latency). На основі цих даних пристрій

отримує статус: "Добрий" (стабільний зв'язок), "Середній" (висока затримка) або "Поганий" (втрата пакетів), що є раннім виявленням деградації з'єднання.

Для фіксації повних відмов, система використовує поріг очікування (наприклад, 3 цикли сканування). Якщо пристрій, що раніше був у мережі, не відповідає протягом заданого часу, його відмова реєструється у журналі сповіщень. Для візуалізації історії стану було інтегровано графіки (Matplotlib), а для полегшення ідентифікації — механізм збереження псевдонімів пристроїв у зовнішньому файлі (devices.json). Це дозволяє користувачеві відрізнити, наприклад, "Роутер у вітальні" від "Xiaomi Inc."

Отримані результати підтвердили доцільність та ефективність використання багаторівневого L3-моніторингу. Запропонований підхід забезпечує збалансованість між точністю детекції, швидкістю оновлення даних та мінімальними ресурсними витратами, що робить його високоефективним для практичного застосування.

Висновки

1. Запропонований метод моніторингу доступності IoT-пристроїв, реалізований як настільний програмний засіб, забезпечує своєчасне виявлення як повних відмов (тайм-аут), так і часткових (деградація каналу, втрата пакетів).

2. Використання ICMP-протоколу (ping) у поєднанні з автоматичним визначенням мережі (через psutil/socket) дозволило створити гнучке рішення, здатне працювати в різних локальних мережах без втручання користувача.

3. Розроблений desktop-інтерфейс (CustomTkinter) та табличне представлення (ttk.Treeview) спрощують процес моніторингу. На відміну від веб-рішень, даний підхід має прямий низькорівневий доступ до мережевих ресурсів (завдяки scapy), необхідний для L3 діагностики.

4. Інтеграція журналу відмов, візуалізації історії (Matplotlib) та механізму псевдонімів надає користувачу повний набір інструментів для діагностики стану мережі.

5. Подальші дослідження слід спрямувати на розширення методу для виявлення відмов рівня L4/L7 (автоматичний моніторинг сервісних портів) та аналіз безпекових аномалій (автоматичне створення "відбитків" пристроїв).

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Chen H., Zhang X. IoT Device Monitoring and Fault Detection. – Journal of Network Systems, 2022.
2. Sharma V., Gupta A. Real-time Monitoring and Failure Prediction in Local Area IoT Networks using Ping-based Diagnostics. – International Conference on Smart Devices and Systems (ICSDDS), 2023.
3. Zhu L., Wang J. Low-cost and Lightweight Network Availability Checking for Home IoT Environments. – IEEE Transactions on Consumer Electronics, vol. 68, no. 1, 2022.
4. Smith J., Brown P. A Web-based Tool for Local Network Device Status and Health Reporting. – European Journal of Computer Science and Engineering, 2024.
5. Lee K., Kim D. Performance Evaluation of ICMP-based Monitoring Systems for Heterogeneous IoT Devices in LAN. – Journal of Communications and Networks, vol. 24, no. 5, 2022.

Атаманиук Назар Романович — студент групи 1KI-24M, факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: nazik.igrek@gmail.com

Богомолов Сергій Віталійович, к.т.н., доцент каф. ОТ, Вінницький національний технічний університет, м. Вінниця, e-mail: bogomolovsergiy@vntu.edu.ua

Atamaniuk Nazar R. — student of group 1KI-24M, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: nazik.igrek@gmail.com

Bohomolov Serhii, PhD, Associate Professor of Computer Engineering, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: bogomolovsergiy@vntu.edu.ua