УДК 004.78:004.05

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

Атаманюк Н. Р. ;[1] Богомолов С.В., к.т.н., доц.[2]
[1,2]Вінницький національний технічний університет
[1,2]Україна, Вінниця
[1]nazik.igrek@gmail.com; [2]bogomolovsergiy@vntu.edu.ua

Анотація. *У роботі розглянуто метод та програмний засіб моніторингу доступності IoT-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*: IoT; моніторинг; локальна мережа; виявлення відмов; настільний застосунок; ICMP; Scapy; L3-моніторинг; деградація каналу.*

Вступна частина. Як відомо [1], базовим методом моніторингу стану пристроїв у мережі є ICMP, зокрема Echo-Request. Цей метод відноситься до мережевого рівня L3 моделі OSI, оскільки він визначає лише мережеву доступність вузла — тобто, чи підключений пристрій до мережі та чи здатний він відповідати. Але на практиці, як правило, цей метод використовується ізольовано, без врахування стану сервісів на транспортному рівні L4 [2]. Так, для пристрою, успішна відповідь на Ping (L3) створює "ілюзію працездатності", хоча його критичні сервіси (L4) можуть не працювати.

Наприклад, IP-камера може бути "онлайн", але її веб-інтерфейс або RTSP-потік (порт 554) можуть бути "завислими" і не відповідати на TCP-запити. Може бути важко діагностувати таку проблему, оскільки розуміння поведінки пристрою вимагає глибокого розуміння його очікуваних L4-сервісів. Це призводить до ситуації, коли система моніторингу повідомляє про норму, в той час як користувач вже зіткнувся з прихованою відмовою сервісу.

Зараз багато локальних мереж стрімко наповнюються пристроями "Інтернету речей" (IoT), такими як IP-камери, сенсори, "розумні" розетки та реле. Це створює нову проблему: більшість цих пристроїв є "чорними скриньками" (black boxes), які не підтримують традиційні методи глибокого моніторингу, такі як SNMP або встановлення "агентів" (наприклад, Zabbix Agent) [3]. А це потребує побудови нових, безагентних методів моніторингу, здатних оцінювати стан пристрою на обох рівнях, L3 та L4, для виявлення прихованих відмов.

Метою дослідження є розробка та апробація комплексного методу моніторингу IoT-пристроїв, що поєднує аналіз L3-доступності з аналізом L4-сервісів на основі "методу еталонів", для виявлення як мережевих, так і сервісних відмов та безпекових аномалій.

Основна частина. На теперішній час, відома модель моніторингу L3, що базується на ICMP , є недостатньою, оскільки вона не враховує стан сервісів на транспортному рівні L4 та створює "ілюзію працездатності". Беручи це до уваги, у якості методології для виявлення

відмов IoT-пристроїв пропонується комплексний дворівневий L3/L4 аналіз на основі "еталонів" сервісів (фінгерпринтингу).

Для апробації методу було розроблено програмний засіб та проведено тестування на стенді, що складався з 4-х типових мережевих пристроїв. На відміну від статистичних тестів, для виявлення "аномалій" (відмов) ми використовували метод порівняння з "еталоном" для L4 (створеним під час автоматичної фази "Навчання") та метод порогового спрацювання для L3 (failure_threshold).

Стабільна робота характеризується відповідністю поточного L4-сканування збереженому "еталону". Якщо ж L3-статус "Добрий", але виявлено відсутність очікуваного порту, то це "Сервісна відмова L4". Якщо ж L3-статус "Добрий", але виявлено наявність нового, несанкціонованого порту, то у цьому разі фіксується "Безпекова аномалія L4".

Застосовуючи побудований метод на тестовому стенді, ми успішно ідентифікували 3 з 3 ключових сценаріїв. Була миттєво зафіксована як Сервісна відмова L4 (імітація зупинки веб-сервера), так і Безпекова аномалія L4 (імітація запуску Telnet-сервісу). Також була коректно, з урахуванням порогу, зафіксована Мережева відмова L3 (фізичне вимкнення пристрою).

Висновки. В роботі було розроблено комплексний метод та програмний засіб моніторингу IoT-пристроїв для автоматизованого виявлення мережевих (L3) та сервісних (L4) відмов з уникненням проблеми "ілюзії працездатності", властивої традиційним L3-методам (Ping). Результат застосування (апробації) розробленого програмного засобу показує високу точність та надійність у виявленні всіх трьох класифікованих типів відмов, а також показує доцільність застосування "методу еталонів" (фінгерпринтингу) для ефективного безагентного моніторингу "чорних скриньок" IoT. В подальшому планується розширювати функціонал засобу, додаючи підтримку моніторингу UDP-сервісів та інтеграцію з зовнішніми системами сповіщень.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Lyon, G. F. (2009). *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Nmap Project.
[2] Hanes, D., Salgueiro, G., Grossetete, P., & Barton, R. (2017). *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things*. Cisco Press.
[3] O'Farrell, J. (2018). *Python for Network Engineers: The A-to-Z Guide for Network Automation*. Createspace Independent Publishing Platform.

Atamaniuk N. R., Bogomolov S.V.

A method and toolset for monitoring iot devices in local networks with failure detection

Abstract. This paper examines a method and software toolset for monitoring the availability of IoT devices in local networks for timely failure detection. The proposed approach is based on hybrid L3 diagnostics, which includes the periodic sending of 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 in Python, which automatically determines the current network parameters and allows the user to track device statuses in real-time, identify them, visualize status history on graphs, and receive operational notifications in a failure log. This increases the operational reliability of a "smart" network through comprehensive and rapid diagnostics.

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