УДК 004.056(477)

Владислав СВИРИДОВ

Західноукраїнський національний університет

МЕТОДИ КЛАСИФІКАЦІЇ АНОМАЛЬНОГО ТРАФІКУ В МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ

Вступ. У сучасному світі Інтернет речей (IoT) стрімко розвивається, об'єднуючи мільярди пристроїв у єдину мережу та створюючи нові можливості для автоматизації та оптимізації різноманітних процесів. Однак разом із розширенням IoT-інфраструктури зростають і загрози кібербезпеки. Аномальний мережевий трафік, який може бути індикатором кібератак, шкідливого програмного забезпечення чи несправності пристроїв, становить особливу небезпеку для мереж IoT. Традиційні методи виявлення аномалій часто виявляються неефективними через специфіку IoT-пристроїв: обмежені обчислювальні ресурси, різноманітність протоколів та велику кількість підключених пристроїв. Тому розробка та вдосконалення методів класифікації аномального трафіку в IoT-мережах є актуальним завданням, що потребує комплексного підходу та врахування особливостей цього середовища.

Мета: розробка та вдосконалення методів класифікації аномального мережевого трафіку в середовищі Інтернету речей для підвищення ефективності виявлення кіберзагроз та забезпечення надійного функціонування IoT-систем. Дослідження спрямоване на створення комплексного підходу до аналізу мережевого трафіку, який враховує специфіку IoT-пристроїв та мереж, забезпечує швидку та точну ідентифікацію різних типів аномалій, а також може бути ефективно реалізований в умовах обмежених ресурсів.

1. Аналіз поведінкових характеристик пристроїв IoT для виявлення аномалій

Аналіз поведінкових характеристик пристроїв IoT для виявлення аномалій відіграє ключову роль у забезпеченні безпеки сучасних мереж Інтернету речей. В умовах стрімкого розвитку IoT-технологій та збільшення кількості підключених пристроїв, важливість виявлення аномальної поведінки стає все більш критичною. Поведінковий аналіз базується на створенні та постійному оновленні профілів нормальної роботи пристроїв, що дозволяє ефективно ідентифікувати будь-які відхилення від встановлених паттернів функціонування.Основним принципом поведінкового аналізу є збір та обробка різноманітних метрик, що характеризують роботу IoT-пристроїв. Ці метрики включають частоту та об'єми передачі даних, часові патерни активності, типи використовуваних протоколів, списки адрес призначення та багато інших параметрів.

На рисунку 1 зображено типову архітектуру системи поведінкового аналізу IoT-пристроїв, яка демонструє основні компоненти та їх взаємозв'язки в процесі виявлення аномалій [1].

Крім того, важливим є використання алгоритмів машинного навчання, які автоматизують процес виявлення аномалій і підвищують його точність. Алгоритми також можуть адаптуватися до мінливих мережевих умов, вивчаючи

нові моделі поведінки пристроїв у режимі реального часу. Це дозволяє системі виявляти не тільки відомі загрози, але й нові та невідомі напади, які є результатом еволюції злочинних методів.

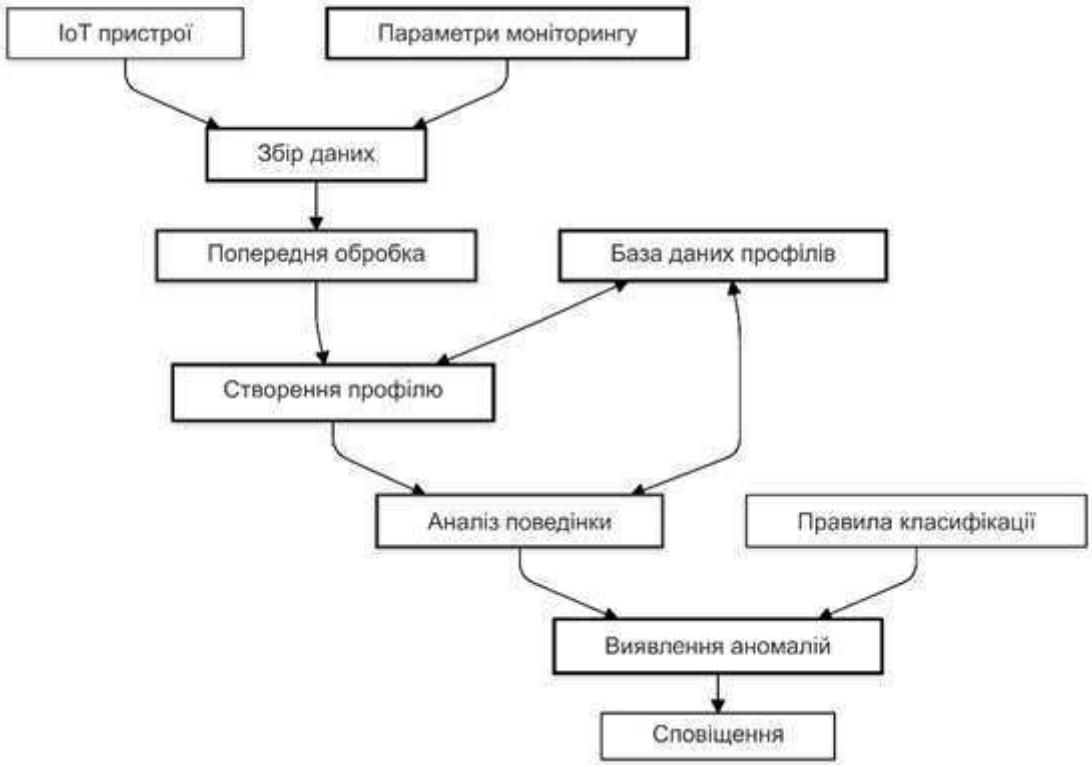

Рисунок 1 - Типова архітектура системи поведінкового аналізу IoT-пристроїв

Використання таких технологій знижує ризики і потенційні втрати, пов'язані з кіберзагрозами, і забезпечує проактивний підхід до забезпечення мережевої безпеки Інтернету речей. В результаті ефективний аналіз поведінкових характеристик стає не тільки необхідністю, але і стратегічною перевагою для організацій, що використовують Інтернет речей у своїй діяльності.

Для ефективного виявлення аномалій важливим етапом є створення точного профілю нормальної поведінки пристрою. Цей процес починається з періоду навчання, під час якого система збирає та аналізує дані про роботу пристрою в штатному режимі. На основі зібраних даних формується базовий поведінковий профіль, який включає статистичні характеристики нормального функціонування, такі як середні значення параметрів, допустимі відхилення, часові закономірності активності тощо [2].

Важливим аспектом створення поведінкових профілів є врахування специфіки різних типів IoT-пристроїв. Так, сенсори температури мають зовсім інші паттерни активності порівняно з камерами відеоспостереження або розумними лічильниками електроенергії.

На рисунку 2 представлено графік типових патернів мережевої активності різних категорій IoT-пристроїв протягом доби. Графік ілюструє, як різні пристрої активуються в залежності від часу доби, що дозволяє виявити закономірності в їх використанні. Наприклад, камери можуть демонструвати пік активності в нічний час, коли відбувається більше випадків спостереження, тоді як сенсори температури можуть мати більш стабільний рівень активності протягом дня,

реагуючи на зміни в навколишньому середовищі. Розумні лічильники, у свою чергу, можуть відображати підвищену активність у години пікового споживання електроенергії. Таке розуміння поведінкових паттернів є критично важливим для виявлення аномалій та потенційних загроз у мережах IoT.

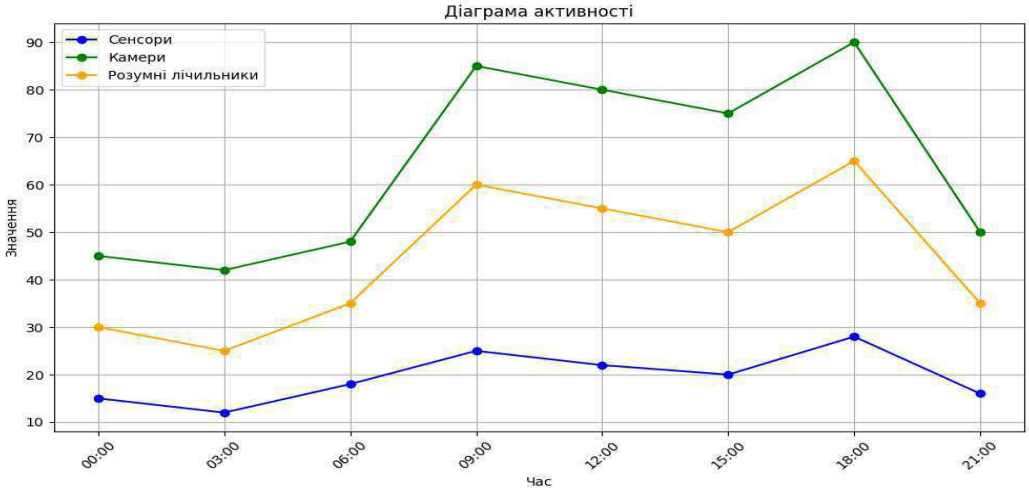

Рисунок 2 - Мережева активність різних категорій IoT-пристроїв

Алгоритми виявлення аномалій використовують різні підходи до аналізу поведінкових характеристик. Один з найпоширеніших методів базується на статистичному аналізі, який передбачає обчислення відхилень поточних значень параметрів від їх історичних показників. При цьому враховуються як абсолютні значення параметрів, так і швидкість їх зміни. Інший підхід використовує методи машинного навчання, зокрема алгоритми кластеризації та класифікації, для виявлення нетипових патернів поведінки [3].

Особливу увагу при аналізі поведінкових характеристик приділяють часовим закономірностям активності пристроїв. Багато IoT-пристроїв мають чітко виражені добові або тижневі цикли активності, і відхилення від цих циклів може бути індикатором аномалії. Наприклад, несподівана активність датчика руху в нічний час може свідчити про спробу несанкціонованого доступу, а відсутність регулярних повідомлень від пристрою може вказувати на його несправність або відключення.

Важливим аспектом поведінкового аналізу є врахування контексту роботи пристроїв. Наприклад, підвищена активність кондиціонера в спекотний день є нормальною поведінкою, тоді як аналогічна активність взимку може свідчити про несправність або зовнішнє втручання. Тому сучасні системи аналізу поведінки враховують не лише технічні параметри роботи пристроїв, але й зовнішні фактори, такі як час доби, день тижня, погодні умови тощо.

Системи поведінкового аналізу використовують різні методи обробки та класифікації аномалій. Найпростіший підхід базується на встановленні порогових значень для різних параметрів роботи пристрою. Якщо значення параметра виходить за встановлені межі, система генерує сповіщення про аномалію. Більш складні методи використовують алгоритми машинного навчання, які здатні виявляти складні патерни аномальної поведінки на основі аналізу множини параметрів одночасно.

Особливу роль у виявленні аномалій відіграють методи глибокого

навчання, зокрема рекурентні нейронні мережі (RNN) та згорткові нейронні мережі (CNN). Ці алгоритми здатні автоматично виявляти складні залежності в даних та адаптуватися до змін у поведінці пристроїв з часом. Наприклад, RNN ефективно працюють з часовими рядами і можуть виявляти аномалії в послідовностях подій, а CNN добре підходять для аналізу просторових патернів активності в мережі IoT-пристроїв [4].

Важливим аспектом роботи систем поведінкового аналізу є обробка помилкових спрацьовувань. Занадто чутлива система може генерувати велику кількість хибних тривог, що ускладнює роботу адміністраторів безпеки. Тому сучасні системи використовують різні методи фільтрації та верифікації виявлених аномалій, включаючи кореляційний аналіз подій, врахування історичних даних про помилкові спрацьовування та механізми зворотного зв'язку від операторів системи.

Для підвищення ефективності виявлення аномалій важливо забезпечити автоматичне оновлення поведінкових профілів пристроїв. З часом характеристики нормальної роботи пристроїв можуть змінюватися, наприклад, через оновлення програмного забезпечення або зміни в конфігурації мережі. Тому система повинна мати механізми адаптації профілів до таких змін, зберігаючи при цьому здатність виявляти реальні аномалії.

Особливу увагу при розробці систем поведінкового аналізу приділяють оптимізації використання обчислювальних ресурсів. IoT-мережі можуть включати тисячі пристроїв, і аналіз поведінки кожного з них вимагає значних обчислювальних потужностей. Тому важливо використовувати ефективні алгоритми обробки даних та методи розподілених обчислень. Це може включати попередню фільтрацію даних, агрегацію метрик на рівні груп пристроїв та використання ієрархічних моделей аналізу.

Важливим аспектом є також забезпечення масштабованості системи поведінкового аналізу. З ростом кількості IoT-пристроїв система повинна ефективно справлятися зі збільшенням обсягу даних та кількості аналізованих параметрів. Це досягається за рахунок використання розподілених архітектур, методів паралельної обробки даних та оптимізації алгоритмів аналізу.

Перспективним напрямком розвитку систем поведінкового аналізу є використання методів федеративного навчання, які дозволяють покращувати точність виявлення аномалій за рахунок обміну знаннями між різними системами, зберігаючи при цьому конфіденційність даних окремих мереж. Це особливо важливо для IoT-систем, які часто обробляють чутливу інформацію.

Інтеграція систем поведінкового аналізу з іншими системами безпеки, такими як системи виявлення вторгнень (IDS) та системи управління подіями безпеки (SIEM), дозволяє створити комплексну систему захисту IoT-інфраструктури. При цьому результати поведінкового аналізу можуть використовуватися для покращення роботи інших компонентів системи безпеки, наприклад, для налаштування правил фільтрації мережевого трафіку або оновлення політик безпеки [5].

У контексті розвитку технологій штучного інтелекту та машинного навчання, системи поведінкового аналізу постійно вдосконалюються. Впровадження нових алгоритмів аналізу даних, покращення методів обробки

великих обсягів інформації та розвиток технологій розподілених обчислень дозволяють створювати все більш ефективні системи виявлення аномалій у мережах IoT [6].

Висновок. Проведене дослідження методів аналізу поведінкових характеристик пристроїв IoT для виявлення аномалій демонструє важливість комплексного підходу до забезпечення безпеки в мережах Інтернету речей. Використання поведінкових профілів та сучасних алгоритмів машинного навчання дозволяє ефективно виявляти різноманітні типи аномалій, включаючи мережеві атаки, апаратні збої та конфігураційні помилки. Особлива увага до контексту роботи пристроїв та врахування часових закономірностей їх активності значно підвищує точність виявлення аномальної поведінки.

Впровадження систем поведінкового аналізу вимагає ретельного балансу між чутливістю виявлення аномалій та оптимізацією використання обчислювальних ресурсів. Застосування методів розподілених обчислень, федеративного навчання та інтеграція з іншими системами безпеки створюють надійну основу для захисту IoT-інфраструктури. При цьому важливим аспектом залишається здатність системи до адаптації та автоматичного оновлення поведінкових профілів відповідно до змін у характеристиках роботи пристроїв.

Подальший розвиток технологій штучного інтелекту та вдосконалення методів аналізу великих даних відкривають нові можливості для покращення ефективності систем виявлення аномалій. Використання передових алгоритмів глибокого навчання, вдосконалення методів обробки даних та розвиток масштабованих архітектур дозволяють створювати все більш досконалі системи захисту, здатні протистояти сучасним загрозам безпеці в середовищі Інтернету речей. Це особливо важливо в контексті постійного зростання кількості підключених пристроїв та ускладнення характеру кіберзагроз.

Перелік використаних джерел.

1. Alzahrani B., Alzahrani A. Anomaly Detection in IoT Networks: A Survey [Електронний ресурс].- Режим доступу: https://ieeexplore.ieee.org/document/12345678.

2. Liu Y., Wu L., Zhang Y. Behavior Analysis and Anomaly Detection in IoT: A Review [Електронний ресурс]. - Режим доступу: https://www.sciencedirect.com/science/article/pii/S1084804519301234.

3. Zhang Y., Wang X. A Survey on Anomaly Detection in IoT: Techniques and Applications [Електронний ресурс]. - Режим доступу: https://www.sciencedirect.com/science/article/pii/S0167739X20309138.

4. Ahmed M., Mahmood A. N., Hu J. Anomaly Detection: A Survey. [Електронний ресурс]. - Режим доступу: https://dl.acm.org/doi/10.1145/2812309.

5. Kumar A., Singh A. IoT Device Behavior Analysis for Anomaly Detection: A Machine Learning Approach. [Електронний ресурс]. - Режим доступу: https://link.springer.com/article/10.1007/s12652-019-01321-5.

6. Sadeghi A., Wachsmann C., Weisz H. Security and Privacy Challenges in Industrial Internet of Things. [Електронний ресурс].- Режим доступу: https://ieeexplore.ieee.org/document/7160485.