

ВИЗНАЧЕННЯ АНОМАЛЬНИХ СТАНІВ У РОБОТІ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

АЛЕКСЄЄВ М.О., БЕЗЛЮДНОВ Д.Є.

Інститут телекомунікаційних систем НТУУ «КПІ», Україна

E-mail: daniilbezlyudnov@gmail.com

Identifying anomaly states of the devices in IoT

Identifying anomaly states is complex problem that have a lot of different solutions. This paper describes how to detect anomalies in IoT sphere using Elman neural network.

На сьогоднішній день існує безліч розмов з приводу Інтернету речей (IoT). Інтернет речей - концепція комунікаційної мережі фізичних або віртуальних об'єктів, які мають технології для взаємодії між собою та з оточуючим середовищем, а також можуть виконувати певні дії без втручання людини. Дана концепція дозволяє змінити якість життя.

Кількість розумних пристроїв та протоколів їх взаємодії збільшується щодня, але всі ці пристрої працюють на різних платформах, мають різні служби та взаємодіють на основі різних протоколів та ін. Відсутні чітко прописані стандарти у цій сфері, що є причиною безлічі проблем (рис. 1), пов'язаних із сумісністю та нормальною взаємодією цих пристроїв. Існує безліч пристроїв, які через відсутність стандартів та наявності великої конкуренції у цій сфері взаємодіють лише з такими самими пристроями або пристроями, що виготовлені тим самим виробником.

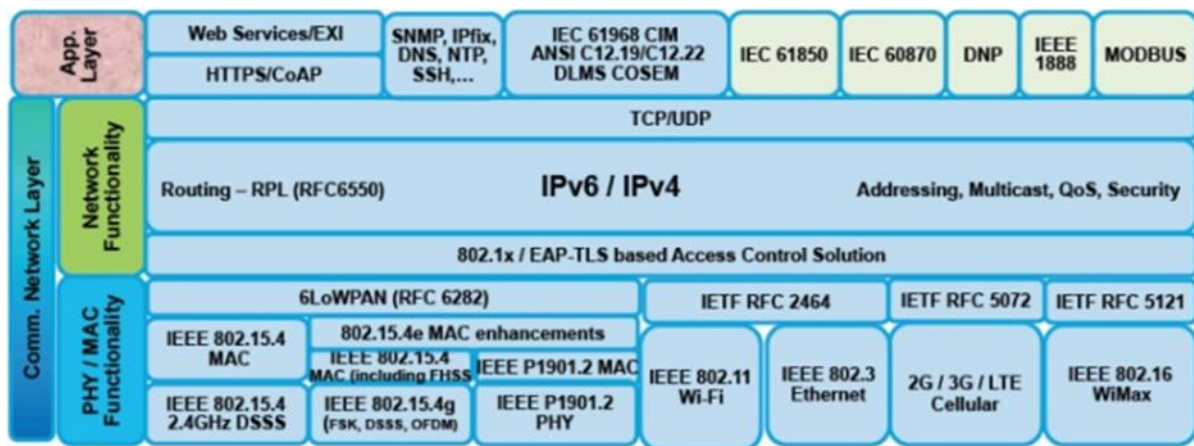


Рис. 1 Стэк протоколів IoT.

Основною проблемою є велика кількість пристроїв, які працюють на абсолютно різних протоколах на всіх рівнях OSI (рис. 1). Різноманітність протоколів зв'язку, невеликі потужності у каналі зв'язку, вплив та нестабільність навколишнього середовища ускладнюють можливість детектування позаштатних ситуацій в режимах роботи пристроїв IoT. Також, негативно впливають на можливість детектування позаштатних ситуацій, великі об'єми даних та дуже часто високі швидкості надходження нових даних.

Якщо розглядати потік даних, то можна виділити наступні види аномалій (рис. 2):

- короткі аномалії;
- різкі зміни константних значень;
- сильні зміни у середньому значенні;
- великі зміни у амплітуді (зміни мінімуму та максимуму);
- непостійні зміни у “формі” або періодичності.

При визначенні аномалій треба виділяти певні “рівні”, чи є дана ситуація аномальна. Який рівень відхилення температури термодатчика від середнього значення можна назвати аномалією? 100%, 50%, 10% чи 1%? Через відсутність чітко визначених критеріїв введемо поняття шкали аномалій.

На шкалі аномалій можна виділити певні основні рівні відхилень:

1. Рівень шуму - рівень незначних відхилень від середніх значень;
2. Рівень змін - рівень на якому в потоці даних детектуються певні зміни, які ще не можна назвати аномальними (рівень перехідних процесів);
3. Рівень аномалій - рівень різких, непередбачуваних змін.

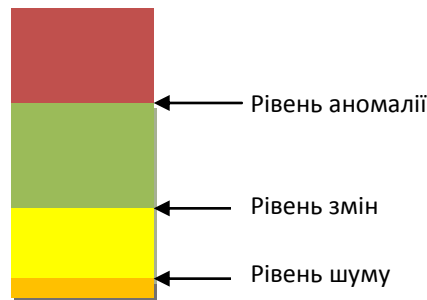


Рис. 2 Шкала аномалій.

Числові, або відсоткові (по відношенню до середнього значення) значення рівнів обираються під конкретні дані.

В середньому, значення по відношенню до середнього значення можна визначити наступними:

1. рівень шуму - 1..5-10%;
2. рівень змін - 11..30-50%;
3. рівень аномалій - >50%.

Детектування аномалій здійснюється за допомогою нейронної мережі Елмана (рис. 3) із блоком пам'яті, яка складається із наступних елементів:

1. Вхід - вхідний рівень перцептронів, кількість яких рівна розмірності вхідних даних (N);
2. Прихований рівень - проміжний рівень перцептронів, кількість нейронів на цьому рівні не менша за $2N$ (N входів та N обернених зв'язків);
3. Вихід - вихідний рівень нейронної мережі, кількість нейронів на цьому рівні може змінюватись від 1 до N;
4. Рівень керування, допоміжний прихований рівень нейронів, кількість нейронів рівна N;
5. Блок пам'яті - в найпростішому рішенні - черга довжиною T.

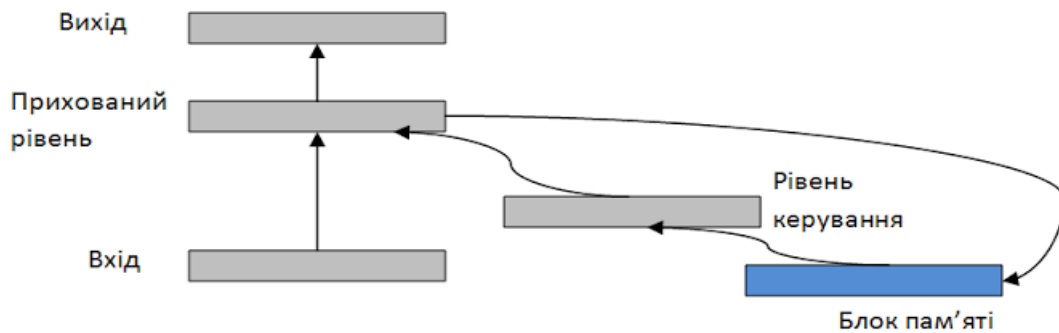


Рис. 3 Структурна схема нейронної мережі Елмана із блоком пам'яті.

Додавання блока пам'яті дає можливість детектувати зміни у порівнянні із попереднім значенням. Для цього раціонально використати від'ємні значення вагів на входах нейронах із рівня керування. Від'ємні значення, затримані на T , підсумовуючись із виходами із вхідного слою дозволяють отримати дельту змін у потоці даних. В якості передаточних функцій використовуються сигмодалльні функції, які дозволяють перейти від бінарних рішень до більш гнучких - відсоткових. Дані від передаточних функцій на вихідному рівні, які лежать у межах від 0 до 1 включно, накладені на певну шкалу можуть визначити із заданою достовірністю, наявність аномалій, змін у потоці даних або їх відсутність.

Запропонований метод детектування аномальних режимів роботи пристроїв IoT є застосовуваним до даної проблеми через:

1. Online`овість роботи, яка витікає у постійному відстежуванні надходжуваних даних, та зберіганні невеликої кількості «історії» даних;

2. Можливість роботи із будь-якими даними через те, що для порівняння використовується функція предикат, яку можна визначити маже на будь яких даних (числові, знакові, текстові, багатовимірні).

3. Простоту, так як метод базується на нейронній мережі Елмана, яка складається із порогових суматорів, зв'язків та блоку пам'яті, як зображено на *рис 3*, які уособлюють собою найпростіші математичні дії.

Проблема пошуку аномальних станів пристроїв досліджується вже давно. Однак розроблені методи погано застосовуються у сфері IoT через велику кількість даних різних типів. Розроблений метод детектування аномальних станів пристроїв IoT є ефективнішим у сфері IoT, ніж інші існуючі через його застосовуваність для будь-яких даних, online`овість та просту реалізацію.

Література

1. Y. Yaoa et al., Online Anomaly Detection for Sensor Systems: a Simple and Efficient Approach, Performance Evaluation, vol 00, pp. 1-24, 2010.
2. S. Rajasegarar et al., "Distributed anomaly detection in wireless sensor networks in conf., ICCS, Florida, USA 2006.
3. B.Abhishek et al., Sensor Faults: Detection Methods and Prevalence in Real-World Datasets, Trans.on Sensor Networks 6(3), 2010.
4. John A. (2015) Recurrent Neural Networks [Online]. Available: https://en.wikipedia.org/wiki/Recurrent_neural_network.