УДК 681.518

Сарапин В.Є., магістрант,
Шабала Є.Є., к.т.н., доцент
Київський національний університет будівництва і архітектури

ГІБРИДНИЙ ПІДХІД ДЛЯ ДІАГНОСТИКИ МЕРЕЖЕВИХ АНОМАЛІЙ ЧЕРЕЗ ПАРАМЕТР ХЕРСТА ТА QOS-МЕТРИКИ

Мережеві відмови є будь-яким порушенням роботи системи, які призводять до зниження продуктивності або повного припинення надання послуг. Для діагностики критично важливо їх класифікувати:

Апаратні відмови – це збої фізичних компонентів (комутатор, кабель, мережева карта) і виявляються через моніторинг стану портів та логів обладнання.

Програмні відмови пов’язані з помилками у мережевому ПЗ, драйверах чи операційній системі пристроїв, які спричиняють непередбачувану поведінку протоколів.

Відмови протоколів з’являються коли несправності пов'язані з некоректною конфігурацією маршрутизації (OSPF, BGP) або транспортних протоколів (TCP-таймаути).

Візантійські відмови вважаються особливим класом відмов, де один або кілька вузлів поводяться зловмисно або непослідовно, надсилаючи суперечливі дані різним частинам розподіленої системи. З позиції мережевої кібербезпеки це може виражатися через:

Для того, щоб встановити нормальний базовий рівень трафіку та спрогнозувати його поведінку використовуються математичні моделі. Моделювання дозволяє відрізнити нормальні коливання навантаження від справжніх аномалій.

Модель Пуассона традиційно використовується для моделювання надходження подій або пакетів. Вона передбачає, що прибуття пакетів є незалежним і відбувається з постійною середньою інтенсивністю. Для варіанту M/G/1 вхідний процес характеризується розподілом Пуассона зі швидкістю надходження повідомлень λ [1] .

Самоподібний (фрактальний) трафік є більш точною моделлю для високошвидкісних мереж. Вона враховує, що сплески трафіку виглядають однаково на різних часових масштабах (від мілісекунд до годин). Моделювання з використанням параметру Херста (H) є критичним для точного прогнозування перевантажень. Якщо $H=0.5$, трафік відповідає моделі Пуассона. Якщо $0.5<H<1$, трафік є самоподібним, що вказує на сильні залежності та довший час перебування в черзі.

Ланцюги Маркова, особливо приховані Марковські моделі, успішно застосовуються для класифікації різних протоколів і типів трафіку [2].

Для моніторингу та діагностики пропонується трирівнева архітектура, що забезпечує масштабованість та поділ відповідальності. Алгоритм використовує поєднання класичного моніторингу QoS та моделі самоподібності для підвищення точності виявлення, особливо для прихованих атак, як-от Slowloris або Low-Rate DDoS, які не завжди викликають різке перевищення традиційних порогів.

Формування базового рівня. Протягом встановленого періоду (наприклад 7 днів) збираються дані QoS-метрик та розраховується середнє значення параметра Херста для трафіку в кожному сегменті. Встановлюються статистичні діапазони нормального функціонування

Розрахунок ознак у реальному часі. Для кожного часового вікна (наприклад 5 секунд) розраховуються поточні значення:

(затримка, втрата пакетів, джитер).

(поточний параметр Херста).

Система виявляє мережеві аномалії завдяки генерації сигналів тривоги типу А, коли поточні показники якості обслуговування виходять за межі статистичного діапазону та сигналів типу Б, якщо зростання параметру самоподібності . Це є показником традиційних несправностей або потенційних прихованих загроз.

Верифікація та кореляція. Сигнали тривоги типу А та Б від різних сенсорів, що відбуваються одночасно, піддаються кореляційному аналізу. Якщо сигнал типу Б походить від вузла, який одночасно надсилає суперечливі дані іншим сенсорам, це підтверджує візантійську відмову або компрометацію.

Список використаних джерел:

1. Моделювання процесів керування у корпоративних комп’ютерних мережах / упоряд. Посашков О. Ю., Безкоровайний В. В. Харків : ХНАДУ, 2021. URL: https://dspace.khadi.kharkov.ua/server/api/core/bitstreams/a6ec3c97-37e3-4e8b-ba0f-651fa0f67e30/content (дата звернення: 18.11.2025).

2. Клюшник В.В., Чернецький Є.В., Онищенко О.В. Ідентифікація трафіку мереж передачі даних у реальному часі. Вісник Приазовського державного технічного університету. Серія: Технічні науки. 2025. Вип. 50. С. 18-24. DOI: https://doi.org/10.31498/2225-6733.50.2025.336234