МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, програмної інженерії та комп'ютерних наук
Кафедра інформаційних технологій

Пояснювальна записка

до кваліфікаційної роботи
другого (магістерського) рівня

на тему **ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ПРОГНОЗУВАННЯ ТРАФІКУ В ІНФОКОМУНІКАЦІЙНИХ СИСТЕМАХ**

Виконав: студент 2 курсу, групи ІПЗ
спеціальності
121 Інженерія програмного забезпечення

Снігур Назар Орестович

Керівник Стрелковська І.В.

Рецензент Л.Г. Пока

Одеса – 2023 рік

ДОВІДКА

кафедри інформаційних технологій про виконану магістерську роботу

студента 2 курсу, ФКПІ та КН групи ІПЗ

Снігура Назара Орестовича
(прізвище, ім'я та по-батькові)

на тему: Порівняльний аналіз методів прогнозування трафіку в інфокомунікаційних системах

Висновок нормоконтролера пояснювальна записка до кваліф. роботи викон. з незначними порушеннями ДСТУ. Виконано згідно з положенням ХНТУ

Нормоконтролер викл. каф. ІТ (науковий ступінь, вчене звання) 15.12.2023 (підпис, дата) [illegible] І.В. (і. б. прізвище)

Висновок відповідального за перевірку на наявність академічного плагіату згідно сертифікатом ID 1015699644 оригінальність роботи підтвердж.

Відповідальна особа викл. каф. ІТ (науковий ступінь, вчене звання) 15.12.2023 (підпис, дата) [illegible] І.В. (і. б. прізвище)

Попередній захист магістерської роботи
студ. Снігура Н. О (прізвище і.б.) проведено «12» 12 2023 р.

Висновки Кваліфікаційна робота виконана у повному обсязі. У роботі проведено порівняльний аналіз та визначено області застосування методів прогнозування трафіку за допомогою лінійної, кубічної та кубічних В-сплайнів. Здобувач має достатню теоретичну підготовку та добре володіє математичним апаратом. Виконана робота магістра відповідає рівню стандартам та рекомендується до захисту

Члени комісії (підпис) д.т.н., проф. Стрелковська І.В. (науковий ступінь, вчене звання, прізвище і.б.)

(підпис) к.т.н., доц. Григор'єва Т.Є. (науковий ступінь, вчене звання, прізвище і.б.)

(підпис) к.т.н, доц, Горбатов В.Є. (науковий ступінь, вчене звання, прізвище і.б.)

МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, програмної інженерії та комп'ютерних наук
Кафедра інформаційних технологій
Освітній рівень другий (магістерський)
Галузь знань 12 Інформаційні технології
Спеціальність 121 Інженерія програмного забезпечення

ЗАТВЕРДЖУЮ
Завідувач кафедри
інформаційних технологій
_____ Т.І. Григор'єва
«25» 09 2023 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ

1. Тема роботи: Порівняльний аналіз методів прогнозування трафіку в інфокомунікаційних системах

Керівник роботи Стрелковська Ірина Вікторівна, д.т.н., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом закладу вищої освіти від «25» 09 2023 року № 1957

2. Строк подання здобувачем роботи 12.12.2023р

3. Вихідні дані до роботи

1. Орієнтуватися на телекомунікаційні мережі, розраховані та осбслуговування пристроїв Інтернету речей
2. Враховувати можливість генерації несанкіонованого трафіку
3. Орієнтуватися на методи сплайн-екстраполяції

4. Зміст пояснювальної записки

1. Методи оцінки трафіку в інфокомунікаційних системах
2. Прогнозування інфокомунікаційного трафіку за допомогою лінійних та кубічних сплайнів
3. Прогнозування інфокомунікаційного трафіку за допомогою кубічних в-сплайнів

5. Перелік демонстраційних креслень: Презентація (10 слайдів).

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Методи оцінки трафіку в інфокомунікаційних системах	9.10.2023-15.10.2023	
2	Прогнозування інфокомунікаційного трафіку за допомогою лінійних та кубічних сплайнів	6.11.2023 – 12.11.2023	
3	Прогнозування інфокомунікаційного трафіку за допомогою кубічних в-сплайнів	20.11.2023 – 26.11.2023	

Здобувач _____ Н.О. Снігур

Керівник роботи _____ І.В. Стрелковська

ВІДГУК КЕРІВНИКА

на кваліфікаційну роботу другого (магістерського) рівня здобувача
Снігура Назара Орестовича
на тему: «Порівняльний аналіз методів прогнозування трафіку в інфокомунікаційних системах»

Якість сервісу, що надається, є одним із головних параметрів інфокомунікаційних систем. Однак сучасний трафік, що створюється пристроями із самим різноманітним функціональним призначенням, значно відрізняється від класичного телефонного трафіку, для прогнозування якого достатньо було використовувати пуасоновські потоки. Таким чином, нові виклики сьогодення потребують пошуку нових методів прогнозування трафіку. У дослідженні, що було проведено в роботі, розглядалися новітні та перспективні методи прогнозування трафіку, зокрема, методи, засновані на використанні різних видів сплайнів, що робить роботу Снігура Н.О. актуальною.

Здобувач Снігур Н.О. повністю виконав завдання до кваліфікаційної роботи. В процесі роботи здобувач Снігур Н.О. працював самостійно. Графік консультацій не порушувався. Поставлене завдання виконано у повному обсязі. Пояснювальна записка та демонстраційні аркуші виконано охайно із дотриманням усіх необхідних вимог.

Під час виконання кваліфікаційної роботи здобувач Снігур Н.О. розібрався з усіма поставленими питаннями та показав уміння користуватись технічною літературою, ставити та розв'язувати дослідницькі задачі.

Кваліфікаційна робота відповідає вимогам до кваліфікаційних робіт другого (магістерського) рівня та заслуговує оцінки «відмінно».

Студент Снігур Н.О. заслуговує присвоєння кваліфікації магістр з інженерії програмного забезпечення за заявленою спеціальністю 121 «Інженерія програмного забезпечення».

Керівник
Декан факультету кібербезпеки
програмної інженерії
та комп'ютерних наук
д.т.н., професор І.В. Стрелковська

відгук керівника

РЕЦЕНЗІЯ

на кваліфікаційну роботу другого (магістерського) рівня здобувача
Снігура Назара Орестовича
на тему: «Порівняльний аналіз методів прогнозування трафіку в інфокомунікаційних системах»

Кваліфікаційна робота здобувача Снігура Н.О. присвячена питанням технологічного розвитку інфокомунікаційних систем, зокрема питанням збереження необхідної якості обслуговування при збільшенні кількості пристроїв Інтернету речей та при виникненні кібератак. У роботі проведено порівняльний аналіз та визначено області застосування методів прогнозування трафіку за допомогою лінійних, кубічних та кубічних B-сплайнів. Практичне значення роботи полягає у можливості використання отриманих результатів у сучасних інфокомунікаційних мережах, що дозволить вивести їх на більш високий якісний рівень.

Здобувач Снігур Н.О. має достатню теоретичну підготовку та добре володіє математичним апаратом, який він застосовував. Кваліфікаційна робота відповідає завданню, в роботі використані усі вихідні дані. Текст роботи послідовний та зрозумілий, оформлення пояснювальної записки та демонстраційних аркушів якісне.

До недоліків роботи слід віднести:

– недостатню увагу приділено іншим методам прогнозування трафіку, наприклад, методам прогнозування за допомогою штучних нейронних мереж;

– недостатню увагу приділено питанням практичної реалізації розглянутих методів прогнозування трафіку.

Проте, зазначені недоліки не знижують цінності виконаної роботи.

У цілому, кваліфікаційна робота Снігура Н.О. відповідає вимогам до випускних кваліфікаційних робіт здобувачів другого (магістерського) рівня та заслуговує оцінки «відмінно».

Студент Снігур Н.О. заслуговує присвоєння кваліфікації магістр з інженерії програмного забезпечення за заявленою спеціальністю 121 «Інженерія програмного забезпечення».

Рецензент
Завідувач кафедри комп'ютерної інженерії
та інноваційних технологій.
к.т.н., доцент Л.Г. Йона

UNICHECK
by Turnitin

Ім'я користувача:
Медики

ID перевірки:
1016013174

Дата перевірки:
17.12.2023 09:59:08 MSK

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
17.12.2023 19:11:13 MSK

ID користувача:
100006215

Назва документа: Снігур диплом(правки)

Кількість сторінок: 60 Кількість слів: 8861 Кількість символів: 67754 Розмір файлу: 1.64 MB ID файлу: 1015699644

28.8%
Схожість

Найбільша схожість: 3.79% з Інтернет-джерелом (http://dspace.onua.edu.ua/bitstream/handle/11300/26633/Spline-extra.

28.6% Джерела з Інтернету	956	Сторінка 62
3.36% Джерела з Бібліотеки	28	Сторінка 75

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

2.07%
Вилучень

Деякі джерела вилучено автоматично (фільтри вилучення: кількість знайдених слів є меншою за 8 слів та 0%)

0% Вилучення з Інтернету	1	Сторінка 76
2.07% Вилученого тексту з Бібліотеки	3	Сторінка 76

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	8

рецензія

РЕФЕРАТ

Текстова частина магістерської роботи містить 45 с., 6 рис., 3 табл., 34 джерела, 2 додатки.

КЛЮЧОВІ СЛОВА: ІНТЕРНЕТ РЕЧЕЙ, КІБЕРАТАКИ, DDOS-АТАКИ, ПРОГНОЗУВАННЯ ТРАФІКУ, САМОПОДІБНИЙ ТРАФІК, ЕКСТРАПОЛЯЦІЯ, СПЛАЙН-ФУНКЦІЇ, ЛІНІЙНИЙ СЛАЙН, КУБІЧНИЙ СПЛАЙН, КУБІЧНИЙ В-СПЛАЙН

Об'єкт дослідження – процеси передачі інформації в інфокомунікаційних системах.

Предмет дослідження – математичні моделі для прогнозування трафіку в інфокомунікаційних системах.

Мета роботи – визначення методів прогнозування трафіку, придатних для використання в інфокомунікаційних системах.

Метод дослідження – методи математичного аналізу, методи теорії зв'язку.

У роботі виконано аналіз методів прогнозування трафіку в інфокомунікаційних системах. Розглянуті питання прогнозування трафіку в системах Інтернету-речей та при виникненні кібератак. Виконано порівняльний аналіз методів прогнозування трафіку на основі лінійних, кубічних та кубічних В-сплайнів. Проведено моделювання та обчислено похибку екстраполяції інфокомунікаційного трафіку.

ABSTRACT

The text part of the master's thesis contains 45 pages, 6 figures, 3 tables, 34 sources, 2 appendices.

KEYWORDS: INTERNET OF THINGS, CYBEATTACKS, DDOS ATTACKS, TRAFFIC FORECASTING, SELF SIMILAR TRAFFIC, EXTRAPOLATION, SPLINE FUNCTIONS, LINEAR SPLINE, CUBIC SPLINE, CUBIC B-SPLINE

The object of the research is information transfer processes in information communication systems.

The subject of research is mathematical models for traffic forecasting in information communication systems.

The purpose of the work is to determine traffic forecasting methods suitable for use in information communication systems.

Research method is methods of mathematical analysis, methods of communication theory.

The work analyzes traffic forecasting methods in information communication systems. Issues of traffic forecasting in Internet of Things systems and in the event of cyber-attacks are considered. A comparative analysis of traffic forecasting methods based on linear, cubic and cubic B-splines was performed. The simulation was carried out and the extrapolation error of information communication traffic was calculated.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАК

D2D	(Device to Device) – прямий зв'язок між двома пристроями
eMBB	(Enhanced Mobile BroadBand) – розширений мобільний широкосмуговий зв'язок
mMTC	(Massive Machine-Type Communications) – масовий міжмашинний зв'язок
NB-IoT	(Narrowband Internet of Things) – вузькополосний Інтернет речей
QoS	(Quality of service) – якість сервісу
URLLC	(Ultra-Reliable Low Latency Communication) – наднадійний міжмашинний зв'язок
IoT	(Internet of Things) –Інтернет речей
M2M	(Machine to Machine) – міжмашинна взаємодія

ВСТУП

Основним напрямком технологічного розвитку мереж мобільного зв’язку сьогодні є орієнтація на збільшення обсягів мереж інтернету речей (Internet of Things, IoT), що функціонує за принципами міжмашинної взаємодії (Machine to Machine, M2M). Сучасні пристрої IoT використовують широкий набір бездротових технологій зв’язку, найбільш популярними з яких є Wi-Fi (стандартів IEEE 802.11n/ac/ad), ZigBee і Bluethoth (стандартів IEEE 802.15), а також мережі мобільного зв'язку технологій LoRaWan (Low-power Wide-area Network) і NB-IoT (Narrow Band) четвертого покоління 4G/LTE і технологію NR (New Radio) п'ятого покоління 5G. Особливістю побудови архітектури мережі IoT є використання архітектури AdHoc/Mash, які засновані на самоорганізації і використанні технологій віртуалізації, в тому числі і хмарних.

Трафік, який генерується об'єктами мережі IoT, відрізняється великою різноманітністю, починаючи від аперіодичного обміну невеликими за розмірами пакетами, що генерують, наприклад, датчики моніторінгу стану довколишнього середовища, і закінчуючи тривалими сеансами викокошвидкісного зв’язку, що створюють, наприклад, веб-камери. Це означає, що інфокомунікаційні системи, розраховані на обслуговування телефонних абонентів за класичними пуасоновськими потоками, через наявність «сплесків» інформаційного навантаження можуть не забезпечувати необхідну якість обслуговування, що може призвести до втрат важливої інформації, клієнтів інфокомунікаційних компанії.

Поточна ситуація ускладнюється зростанням несанкціонованого трафіку, який виникає, наприклад, у випадках кібератак зловмисників, кількість яких збільшується з кожним роком.

Усе це потребує розробки та розробки та впровадження нових методів прогнозування інфокомунікаційного трафіку, які б враховували актуальні потреби

сьогодення та забезпечували необхідний рівень сервісу клієнтів інфокомунікаційних компаній.

Це і обумовило мету даної роботи, яка полягає у дослідженні нових методів прогнозування трафіку, придатних для використання в інфокомунікаційних системах, розрахованих на масове застосування пристроїв Інтернету речей в умовах постійно зростаючої кількості кібератак.

1 ОСОБЛИВОСТІ ТРАФІКУ В ІНФОКОМУНІКАЦІЙНИХ СИСТЕМАХ

1.1 Особливості трафіку в мережах Інтернету речей

Розвиток інфокомунікаційних мереж відбувається в напрямку підвищення швидкості передачі даних із збереженням необхідної якості обслуговування QoS (Quality of Service). Причиною цього, у першу чергу, є збільшення обсягів мультимедійних та інтерактивних послуг, що потребують кінцеві користувачі. Проте паралельно із цим процесом відбувається також і стале зростання сегменту Інтернет речей IoT (Internet of Things) на базі міжмашинної M2M (Machine to Machine) та D2D (Device to Device) взаємодії, що потребує від інфокомунікаційних мереж інших критеріїв QoS, зумовлених специфікою пристроїв IoT, наприклад, необхідністю жорсткої економії енергії джерела живлення.

Особливістю інфокомунікаційної структури Інтернету речей є здатність до автоматичної самоорганізації, що дозволяє інтернет-речам об’єднуватись в складні мережі без втрати власної віртуальної суб’єктивності [1].

Застосунки IoT відрізняються великою різноманітністю. Наразі, з точки зору інфокомунікацій, їх умовно поділяють за на три доволі великі групи, що відрізняють типом послуг, що надаються:

– застосунки, що потребують мобільного широкосмугового доступу eMBB;

– застосунки масової міжмашинної взаємодії mMTC;

– застосунки, що потребують надійного з'єднання з низькою затримкою часу URLLC.

Для технологічного забезпечення роботи інтернет-речей IoT, що мають малі обсяги інфокомунікаційного трафіку але критичні до швидкості передачі даних та часу затримки пакетів, консорціумом 3GPP запропоновано використання вузькосмугового Інтернету речей NB-IoT (Narrowband Internet of Things), що дозволяє на базі мережі технології LTE надавати для IoT-пристроїв

низькошвидкісні послуги передачі даних до 200 кбіт/с [2] Для забезпечення працездатності M2M-пристроїв масового типу 3GPP рекомендує використовувати технології EC-GSM-IoT (Extended Coverage GSM for IoT), а для M2M-пристроїв зі швидкістю передачі до 1 Мбіт/с – технології LTE-M. Таким чином, різні види пристроїв інтернету-речей генерують різні види інфокомунікаційного трафіку, що відрізняється як швидкістю передачі даних, так і часу передачі пакетів.

Наразі не існує загальноприйнятого підходу та визначених рекомендацій щодо прогнозування трафіку M2M та D2D-пристроїв, в тому числі оптимального методу для розподілу обмеженої кількості інфокомунікаційних радіоресурсів між кінцевими користувачами та IoT-пристроями. Значна кількість досліджень спрямована на дослідження характеристик M2M-трафіку, який має малий розмір переданих блоків даних і велику кількість пристроїв, що підключаються [3], проте питання його загального впливу на інфокомунікаційну мережі ще потребують додаткових досліджень.

Трафік в мережі IoT визначається як об'ємом даних, що передаються кожним пристроєм IoT, так і загальною кількістю підключених до мережі пристроїв. Природно, що тип та об’єм трафіку, що генерують різні типи пристроїв Інтернету речей, істотно відрізняється Але у будь-якому випадку, вимоги до швидкості передачі даних та часу затримки пакетів визначається саме типом IoT.

Наразі немає єдиної методики визначення IoT-трафіку. У відомих роботах в основному розглядаються M2M-пристрої, до яких відносяться будь-які пристрої, здатні функціонувати та передавати дані через інфокомунікаційну мережу без участі людини. Тому надалі під IoT-трафіком будемо розуміти потоки пакетів, згенерованих інтернет-речами, які мають наступні характеристики:

– інтенсивність надходження пакетів (кількість пакетів за одиницю часу);

– середній розмір одного пакету;

– закон розподілу інтервалів часу між сусідніми пакетами.

При цьому, потоки, що створюють інтернет-речі, можуть бути як випадковими, так і детермінованими.

Під якістю обслуговування інфокомунікаційної мережі (QoS) надалі будемо розуміти знатність передавати IoT-трафік, яка може бути визначена конкретними числовими параметрами, головними з яких є:

– пропускна здатність (швидкісний параметр);

– час затримки пакетів (часовий параметр);

– імовірність втрати пакету (імовірнісний параметр).

Особливістю технології межмашинної взаємодії є використання у якості IoT пристроїв із низькою обчислювальною потужністю, що мають обмежену кількість вбудованої пам’яті та жорсткі вимоги до енергоспоживання, що призводить до формування невеликих за розмірами пакетів, які потрібно передавати за максимально короткий термін, оскільки передача даних через бездротові інтерфейси є енерговитратною. Незважаючи та явну обмеженість у обчислювальних ресурсах, функціональності інтернет-речей цілком достатньо для створення різноманітних датчиків, що можуть використовуватися в таких областях як логістика, сільське господарство, моніторинг екологічного середовища, моніторинг стихійних лих тощо. Незважаючи на невелику кількість трафіку, що може згенерувати одна інтернет-річ, їх загальна кількість може виявитися настільки великою, що загальний трафік, створений усіма M2M інтернет-речами може, буде вже буде істотно впливати на якість обслуговування інфокомунікаційної мережі.

Оцінка якості обслуговування інфокомунікаційної мережі додатково ускладняється малим часом передачі одного пакету, що не дозволяє використовувати існуючі методи визначення якості радіоканалів на основі оцінки тривалості розмови або часу його використання. Крім того, незважаючи на ізольованість окремих інтернет-речей, їх активність може виявитися залежною від зовнішніх подій, наприклад, від зміни погодних умов у системах контролю стану довколишнього середовища, що може призводити неперіодичного та неконтрольованого зростання IoT-трафіку. Таким чином, на сьогоднішній день важливо вміти правильно оцінювати IoT-трафік, а також його вплив на якість послуг, що надаються інфокомунікаційними системами.

Більшість робіт, в яких розглядаються питання оцінки трафіку в інфокомунікаційних IoT-мережах, присвячена дослідженню методів щодо запобігання перевантажень базової станції IoT-мережі M2M-трафіком [4 – 12]. Результати таких досліджень дозволяють лише розподіляти доступні частотні та часові ресурси між абонентами телефонії та M2M-пристроями [4].

При дослідженні трафіку, що створюється пристроями інтернету речей, використовується підхід, який базується на аналізі імовірнісно-часових характеристик пристроїв IoT-мережі з урахуванням моделі потоків викликів на основі законів розподілів випадкових величин та часових характеристик. Наприклад, в роботі [5], розглядаються питання динамічного розподілу радіочастотних ресурсів базової станції NB-IoT, коли трафік пристроїв інтернету речей штучно обмежується, а решта пропускної здатності каналів зв'язку залишається доступною тільки для користувачів телефонії. Але у запропонованій моделі надходження запитів на передачу даних від M2M-пристроїв для використовується простий пуассонівський вхідний потік замовлень, що не дозволяє в повній мірі отримати адекватні до реального процесу результати.

В роботі [6] наведено результати дослідження трафіку IoT, за результатами якого автори стверджують, що поява великої кількості IoT-пристроїв призведе до значного збільшення кількості коротких сеансів з'єднань, які стануть домінуючими в мережі, тому дослідження характеристик мережі IoT необхідно проводити саме для коротких з'єднань, не враховуючі тривалі за часом встановлення з'єднання сеанси. Такий підхід може бути прийнятий для групи масових послуг eMTC, або для критичних до затримок URRL послуг. Однак не враховувати передачу відеозображень, відеомоніторінгу та віртуальної реальності, які характеризуються як значною тривалістю з'єднання, так і значним обсягом трафіку, не можна. Таким чином, при дослідженні імовірнісно-часових характеристик трафіку необхідно враховувати всі види з'єднань та усі види трафіку.

В роботі [7] автори пропонують модель гібридного планування пріоритетів заявок для послуг з різними функціями і обмеженнями на характеристики QoS.

Відповідно до цієї стратегії, чутливим до затримок послуг, призначається високий пріоритет, і вони виконуються негайно, а послуги, які нечутливі до затримок, обслуговуються без пріоритету. Аналіз такої моделі обслуговування заявок показав, що її використання призводить до збільшення довжини черги очікування обслуговування. Такий підхід не є новим при дослідженні характеристик якості обслуговування трафіку, однак дозволяє враховувати довжину черги очікування обслуговування.

Всі розглянуті дослідження дозволяють отримати результати щодо характеристик якості обслуговування трафіку IoT в мережі, за різних умов розглядання.

При рішенні поставленого завдання дослідження характеристик якості обслуговування трафіку в мережі IoT/5G, по-перше, необхідно обрати певний вид IoT пристроїв певної групи послуг, визначити їхні характеристики та змоделювати необхідний потік трафіку. На цьому етапі достатньо важливим є визначення відповідних до визначеної моделі потоку значень закону розподілу надходження запитів на встановлення з’єднань, закону розподілу часу обслуговування замовлень та інших характеристик, які дозволять визначити вид системи масового обслуговування.

Отримані значення в першому етапі будуть підґрунтям для подальшого дослідження характеристик якості QoS обслуговування трафіку, яке буде виконано за допомогою прогнозування характеристик якості IoT пристроїв.

Практичне значення отриманих результатів полягає в тому, що за їхніми значеннями буде передбачена відповідна «траса» трафіку, що дозволить отримати необхідний обсяг буферних пристроїв, тим самим уникнути перевантажень IoT пристроїв і перевищень нормативних значень характеристик QoS.

Для дослідження характеристик трафіку в інфокомунікаційних мережах необхідно визначити залежність між обсягом трафіку, що створюється в мережі, з підтримкою характеристик якості обслуговування QoS і параметрами мережі, що забезпечують ефективне використання доступних мережевих ресурсів.

Підтримка певного рівня обслуговування в мережі 5G з метою надання різноманітних мультимедійних послуг потребує вивчення характеристик трафіку. Наприклад, відомо, що високошвидкісний відеотрафік має досить часті та значні «сплески» інтенсивності, що при обслуговуванні призводить до збільшення часу затримки та може істотно впливати на якість обслуговування QoS [8].

Дослідження характеристик якості обслуговування трафіку IoT має наступні особливості:

– потрібно враховувати об'єм даних, що генерується кожним пристроєм IoT, так і їх загальну кількість;

– потрібно враховувати клас послуг IoT (eMBB, mMTC, URLLC), який визначає швидкісні характеристики та значення допустимих затримок в передачі даних;

– потрібно враховувати функціональність пристроїв IoT, наприклад M2M-пристрої здатні відправляти дані через мережу зв'язку і функціонувати без безпосередньої участі людини.

З точки зору особливостей IoT-трафіку слід зазначити його відмінності в залежності від виду датчиків MTC, якщо це телеметричні датчики, датчики передавання даних та інші, що забезпечують низькошвидкісне передавання данних, частіше цей тип IoT-пристроїв обслуговується за допомогою технології NB-IoT LTE. Для мобільних пристроїв IoT, характерні послуги eMBB логістики, розумних сервісів і додатків, послуги медицини, які обслуговуються за допомогою технології LTE-M IoT, а послуги URLLC, до яких відносяться послуги віддаленної хірургічної операції, дрони, камери спостереження, передача HDвідео в реальному масштабі часу, Smart Grid розумні мережі, real-time послуги, тактильний інтернет будуть використовувати технологію NR/5G.

Саме тому, визначення характерстик якості не завжди дозволяє базуватися на результатах тільки визначення характеристик якості QoS, таких як: значення часу затримки та пропускна спроможність.

1.2 Особливості трафіку при наявності кібератак

Стрімкий розвиток інформаційних та інфокомунікаційних технологій сьогодні відбувається практично у всіх сферах діяльності людства, забезпечуючи користувачів можливостями безмежного санкціонованого доступу до інформації, але водночас забезпечує практично необмежені можливості для несанкціонованих, а іноді протиправних дій. Питання забезпечення кібербезпеки сьогодні, за умов стрімкого розвитку технологій, стають стратегічно важливим завданням, особливо щодо економіки, електронної промисловості, електронних комунікацій та державних електронних ресурсів.

Технічний рівень кіберзагроз, постійно зростає та удосконалюється. З кожним роком створюються нові інструменти та механізми кібератак [13]. Тому виникає проблема пошуку нових методів виявлення непередбачених загроз, які ґрунтуватимуться на принципово нових ідеях та математичних рішеннях, що дозволяють покращити відомі результати та протистояти загрозам кібератак.

Одним з ефективних рішень запобігання вторгненням в умовах їх постійного ускладнення та кількісного зростання є засоби моніторингу та багатофункціонального аналізу трафіку. Моніторинг мережного трафіку сьогодні націлений насамперед на оперативне виявлення «сплесків» мережевого трафіку інфокомунікаційної мережі, що є результатом несанкціонованого доступу, вірусів, атак, вторгнень та інших загроз інформаційній безпеці. Серед таких загроз найчастіше зустрічаються атаки типу DDoS (Distributed Denial of Service), які стають все більш інтенсивними та руйнівними, а їхня кількість безперервно зростає. При цьому виявити їх досить важко через значну кількість джерел атак і особливостей трафіку. Характеристики шкідливого трафіку атак іноді можуть бути майже невідмінними від легітимного.

Процес виявлення кібератаки в мережі найчастіше заснований на порівнянні характеристик трафіку на незначному відрізку часу вторгнення з відповідною легітимною трасою трафіку, розглянутої за тривалий період часу. У цьому випадку, якщо виявлено значні «сплески» трафіку, виникає необхідність знайти

такий метод виявлення кібератак, у якому похибка виявлення буде мінімальною. Для протидії зловмисникам сьогодні створено низку складних систем виявлення вторгнень IDS/IPS (Intrusion detection system/Intrusion prevention system), міжмережеві екрани, аналізатори трафіку на базі утиліт та сніферів (tcpdump, Wireshark, Snort), протоколи SNMP (NetFlow). Для оцінки трафіку ці системи використовують різні методи, серед яких: статистичні методи, інтелектуальний аналіз даних, штучний інтелект, вейвлет-аналіз та інші [14 – 21].

Згідно з вищевикладеним слід зазначити, що актуальною є завдання виявлення «сплесків» мережевого трафіку атак типу DDoS (SYN-Flood, ICMP-Flood, UDP-Flood), рішення якої розглянуто у роботах авторів [14 – 21]. Один із широко використовуваних підходів до виявлення DDoS-атак з використанням марківських моделей запропонований у роботі [14]. Використовуючи аналіз шаблонів атаки за допомогою прихованої марківської моделі, отримано прогноз атак, хоча частина трафіку атаки може бути втрачена. У роботі [15, 16] авторами запропоновано метод, заснований на байєсовських мережах, за допомогою якого було покращено прогноз виявлення вторгнень. Такий похід значно ускладнював визначення атаки і при цьому не вдалося уникнути хибних прогнозів. У роботі [16] на основі байєсівської мережі запропоновано раннє прогнозування з використанням кореляції. Проте така реалізація не є універсальною і не дозволяє прогнозувати всі види атак. Для виявлення атак з урахуванням розширеного набору ознак у роботі [17] використано машинне навчання ML/DL. Така реалізація, як правило, вимагає навчання та значних часових витрат. Використання вейвлет-перетворень для визначення DDoS-атак у роботі [18] дозволяє значно покращити результати виявлення та прогнозування загроз. Автори роботи [19] при порівняльному аналізі застосовуваних методів виявили, що метод регресійного дерева кращим для виявлення атак у трафіку 5G. Переваги використання штучного інтелекту обґрунтовані авторами у роботі [20], а способи забезпечення мережевої кібербезпеки у роботах [21, 22].

Раніше авторами в роботах [23 – 27] при вирішенні завдань прогнозування та оцінки станів даних, сигналів та трафіку було запропоновано метод сплайн-

екстраполяції. Використання цього методу дозволило покращити результати прогнозування характеристик трафіку різних застосунків з використанням сплайн-функцій (лінійних, квадратичних, квадратичних B-сплайн, кубічних, кубічних B-сплайн, сплайн Ерміта).

При розгляді характеристик трафіку кібератак DDoS часто відзначаються часті періодичні, короткі і значні «сплески» інтенсивності трафіку, а легітимний трафік має невелику амплітуду пульсацій, які відбуваються протягом тривалого часу. Для прогнозування атак, які характеризуються «сплеском» трафіку, доцільно застосувати метод, заснований на базі сплайн-функцій. Враховуючи, що трафік кібератак має властивості самоподібності [28], сплайн-екстраполяція може бути використана при вирішенні задач виявлення та прогнозування атак DDoS (SYN-Flood, ICMP-Flood, UDP-Flood).

1.3 Висновки за розділом

Результати аналізу трафіку в сучасних інфокомунікаційних системах показує, що прогнозування трафіку за класичними методами на основі пуасоновських потоків може призвести до втрат важливої інформації на зниження якості обслуговування. Тому при розгляді нових методів прогнозування трафіку слід враховувати особливості нових джерел інформації, як санкціонованих, так і несанкціонованих, що додатково підтверджує актуальність даної роботи.

2 ПРОГНОЗУВАННЯ ІНФОКОМУНІКАЦІЙНОГО ТРАФІКУ ЗА ДОПОМОГОЮ ЛІНІЙНИХ ТА КУБІЧНИХ СПЛАЙНІВ

2.1 Виявлення та прогнозування трафіку з використанням сплайн-функцій

Розглянемо трафік на відрізку $[a; b]$, припускаючи, що на аналізованому відрізку $[a; b]$ можливий «сплеск» інтенсивності, визваний збільшенням обсягом передачі інформації IoT пристроями або DDoS атакою, який може призвести до відмови сервера, що надає послуги інфокомунікаційного зв'язку. В іншому випадку, розглядатимемо відрізок трафіку «сплеску», який є останнім на відрізку $[a; b]$. Припустимо, що трафік атаки виявлено на відрізку $[c; d]$, $[c; d] \subset [a; b]$, де $[a; b]$ – досить малий окіл відрізку $[c; d]$ (рис. 2.1).

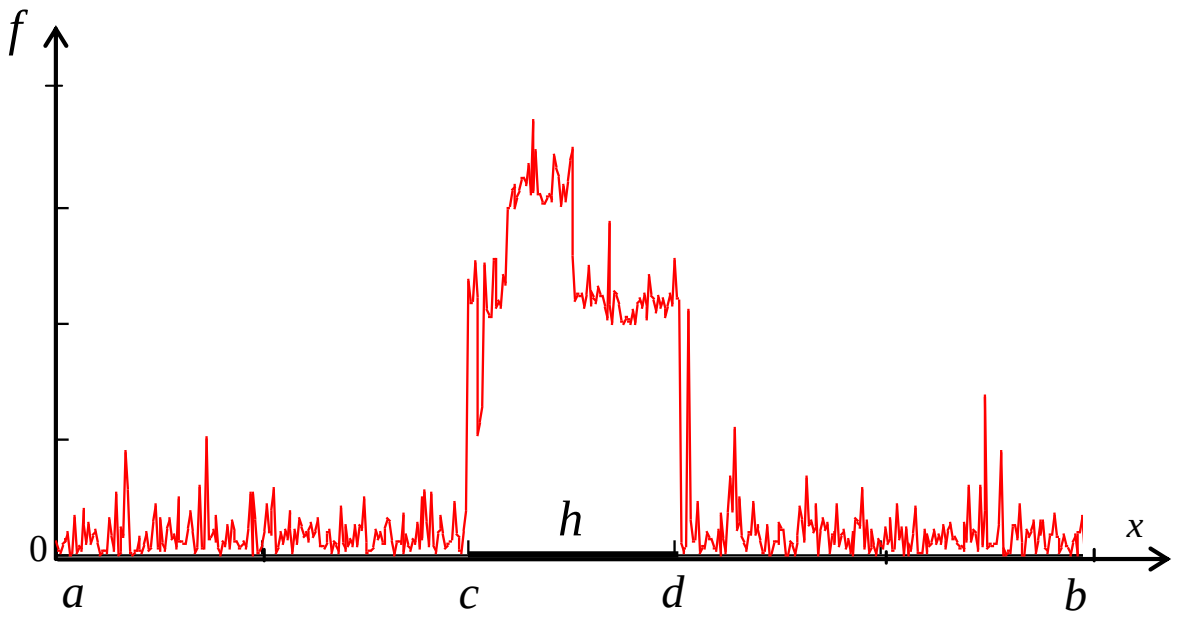


Рисунок 2.1 – Фрагмент інфокомунікаційного трафіку зі сплеском інтенсивності

Нехай на відрізку $[a; b]$ встановлено трафік. Розіб'ємо цей відрізок $[a; b]$ точками Δ: $a = x_0 < x_1 < \ldots < x_N = b$ на проміжки $[x_i, x_i + 1]$, $i = 0, \ldots, N - 1$, на кожному з яких побудуємо багаточлен певного степеню, у якості якого використаємо лінійний сплайн. Відповідно до [29], інтерполяційний лінійний

сплайн $S_1(x_i)$ на відрізку $[x_i, x_{i+1}]$, $i = 0, \ldots, N-1$ – це безперервні шматково-лінійні функції. Інтерполяційний сплайн $S_1(x_i)$ визначається такими умовами [23 – 27]:

$$S_1(x_i) = f_i, \qquad i = 0, \ldots, N. \tag{2.1}$$

Геометрично він є ламаною, що проходить через точки (x_i, y_i), де $y_i = f(x_i)$. Позначимо через $h_i = x_{i+1} - x_i$. Тоді, згідно [29], при $x \in [x_i, x_{i+1}]$, $i = 0, \ldots, N-1$, лінійний сплайн матиме вигляд:

$$S_1(x) = f_i \frac{x_{i+1} - x}{h_i} + f_{i+1} \frac{x - x_i}{h_i}. \tag{2.2}$$

Кубічний інтерполяційний сплайн $S_3(x)$, будується аналогічно лінійному сплайну, з тією різницею, що у кожному проміжку $[x_i, x_{i+1}]$, $i = 0, \ldots, N-1$ це буде кубічна функція. Відповідно до [29], для $x \in [x_i, x_{i+1}]$, $i = 0, 1, \ldots, N-1$ кубічний сплайн має вигляд:

$$\begin{aligned} S_3(x) = {} & f_i(1-t)^2(1+2t) + f_{i+1}t^2(3-2t) + \\ & + m_i h_i t(1-t)^2 - m_{i+1} h_i t^2(1-t) \end{aligned}. \tag{2.3}$$

де $t = \dfrac{x - x_i}{h_i}$, $S_3(x_i) = f_i$, $S_3(x_{i+1}) = f_{i+1}$, $m_i = S'(f; x_i)$.

Для визначення кубічного сплайну виду (2.3) на відрізку $[a; b]$ використовуються граничні умови [22]:

$$S'(f; a) = f'(a), \; S'(f; b) = f'(b). \tag{2.4}$$

Розглядаючи трафік на відрізку $[a; b]$, поставимо рівномірну сітку розбиття з кроком $h_i = h$, $i = 0, 1, \ldots, N-1$, $h = (b - a)/N$. Для побудови лінійних та кубічних сплайнів, визначених вище, використовуємо значення інтенсивності трафіку у вузлах інтерполяції x_i, $i = 0, 1, \ldots, N$. Побудувавши лінійний або кубічний

інтерполяційний сплайн на відрізку [a; b] використовуючи вирази (2.1), (2.2) або (2.3), (2.4), відповідно, отримаємо значення трафіку на відрізку [a; b].

У роботах [23–25] для прогнозування самоподібного трафіку розроблено метод сплайн-екстраполяції. Цей метод дозволяє, використовуючи властивості довгострокової залежності самоподібного трафіку, екстраполювати його значення поза заданим відрізком осі часу. Вибір сплайн-функції при екстраполяції трафіку дозволяє досягти необхідної точності.

Згідно рис. 2.1, трафік атаки виявлено на відрізку [c; d]. Відповідно до [28], що «сплески» трафіку мають властивість самоподібності і, відповідно, характеризується довгостроковою залежністю окремих реалізацій за проміжок часу, схожих як формою, так і візуально. Ступінь самоподібності трафіку визначається значенням параметра Херста $0{,}5 \le H < 1$. Тоді очевидним є те, що при сплайн-екстраполяції «слесків» трафіку слід враховувати значення параметра Херста, попередньо отримане за допомогою R/S-аналізу або ентропійного методу за результатами моніторингу трафіку.

Використовуємо метод сплайн-екстраполяції для прогнозування «сплесків» трафіку, наприклад, кібератак типу DDoS, поза відрізком [a; b]. Прогнозування трафіку поза відрізком [a; b] отримано у роботі [24] на основі методу сплайн-екстраполяції з використанням лінійних або кубічних сплайнів. З огляду на самоподібність трафіку кібератак [28] можна отримати значення прогнозованого трафіку на відрізку [b; p] (рис. 2.2).

Для визначення помилки сплайн-екстраполяції використовуємо такі теореми.

Теорема 1. [29] Якщо сплайн першого ступеня $S_1(x)$ інтерполює неперервну функцію $f(x)$ на сітці Δ, то справедлива оцінка похибки:

$$\left|S_1(x) - f(x)\right| \le \omega(f); \tag{2.5}$$

де $\omega(f)$ – модуль неперервної функції виду

$$\omega(f) = \max_{0 \le i \le N-1} \omega(f) = \max_{0 \le i \le N-1} \; \max_{x'' \in [x_i, x_{i+1}]} |f(x'') - f(x')|.$$

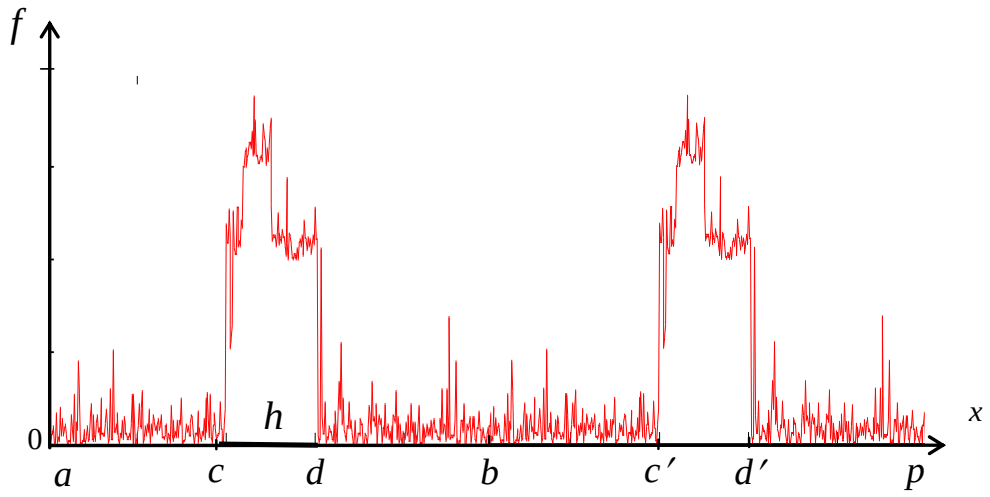


Рисунок 2.2 – Фрагмент інфокомунікаційного трафіку зі «сплеском» інтенсивності на відрізку [*c'*; *d'*]

Теорема 2. [29] Якщо кубічний сплайн $S_3(x)$ інтерполює неперервну функцію $f(x)$ на сітці Δ і задовольняє граничній умові (2.4), тоді:

$$\|S(x) - f(x)\|_C \le \left(1 + \frac{3}{4}\rho\right)\omega(f). \qquad (2.6)$$

де $\rho = \frac{\max_i h_i}{\min_i h_i}$, $\|f(x)\|_C = \max_{x \in [a,b]} |f(x)|$, $C = C[a, b]$ –функція неперервна на інтервалі [a, b].

2.2 Рішення задачі прогнозування трафіку на базі сплайн-екстраполяції з застосуванням лінійних і кубічних сплайнів

Розглянемо сплайн-екстраполяцію трафіку з використанням лінійних та кубічних сплайнів. Для експерименту використовуємо модельований трафік, показаний на рис. 2.1.

Використовуючи лінійний сплайн визначення трафіку на відрізку [1600;1700], виконаємо екстраполяцію трафіку, результати якого показані на рис. 2.3. Неважко бачити, що використання лінійних сплайнів має значну похибку, яка найчастіше з'являється на відрізках трафіку, де інтенсивність атаки трафіку має «сплески».

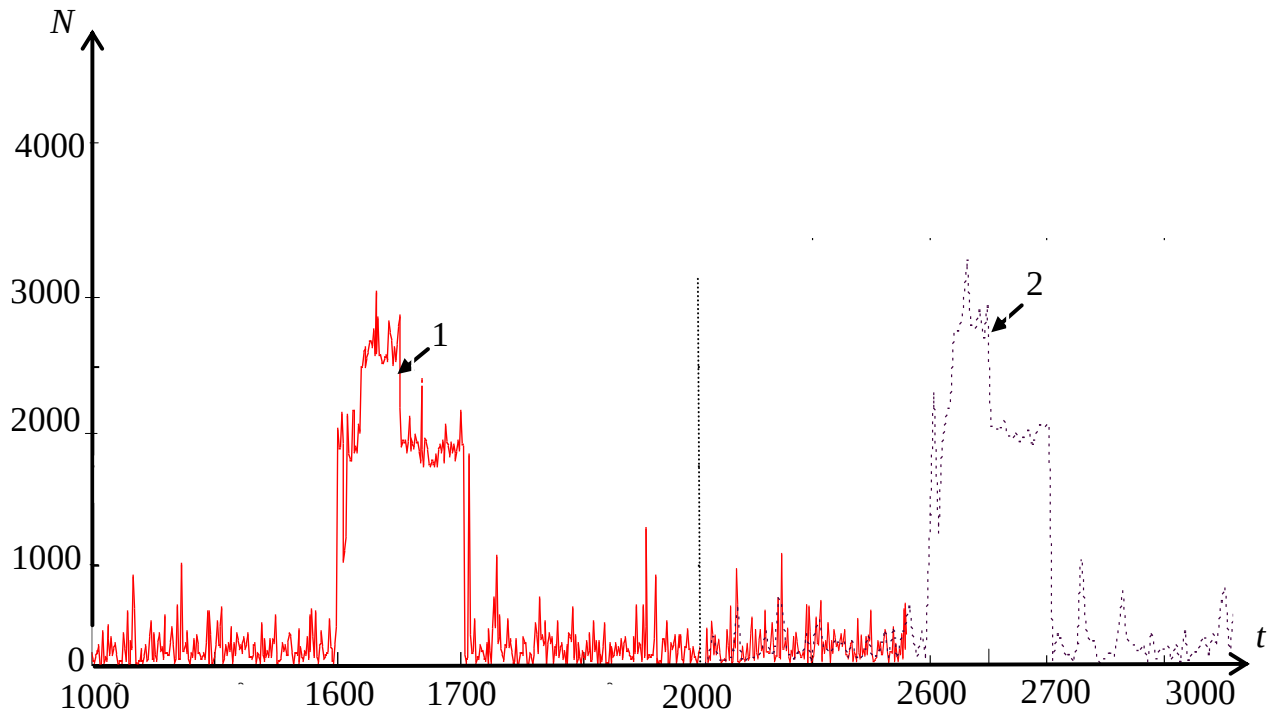


Рисунок 2.3 – Результати екстраполяції інфокомунікаційного трафіку на відрізку [2600;2700] з використанням лінійних сплайнів;
1) «сплеск» трафіку; 2) екстраполяція трафіку з використанням лінійного сплайну.

Для знаходження похибки екстраполяції трафіку за допомогою лінійного сплайну використовуємо формулу (2.5) теореми 1. Результати розрахунку наведено у табл. 2.1.

З табл. 2.1 видно, що точність екстраполяції інфокомунікаційного трафіку дуже мала, тому прогнозувати кібератаку за допомогою лінійних сплайнів недоцільно.

Для зменшення похибки прогнозування кібератаки розглянемо кубічний сплайн виду (2.3), який виявлено на відрізку [1600; 1700]. Аналогічно [17] і

самоподібності трафіку кібератак [28], використовуючи метод екстраполяції, отримаємо «сплеск» трафіку на [2600; 2700] (рис. 2.4).

Таблиця 2.1 – Похибка екстраполяції інфокомунікаційного трафіку за допомогою лінійного сплайну

Проміжок	**Числові значення проміжку, мс**	**Значення похибки**
$[x_0; x_1]$	[2600;2601]	2,6
$[x_1; x_2]$	[2601; 2602]	3,8
$[x_2; x_3]$	[2602; 2603]	0,08
$[x_3; x_4]$	[2603; 2604]	75,6
…	…	…
$[x_{10}; x_{11}]$	[2620; 2621]	27,1
$[x_{11}; x_{12}]$	[2621; 2622]	9,11
$[x_{12}; x_{13}]$	[2622; 2623]	19,6
$[x_{13}; x_{14}]$	[2623; 2624]	2,9
…	…	…

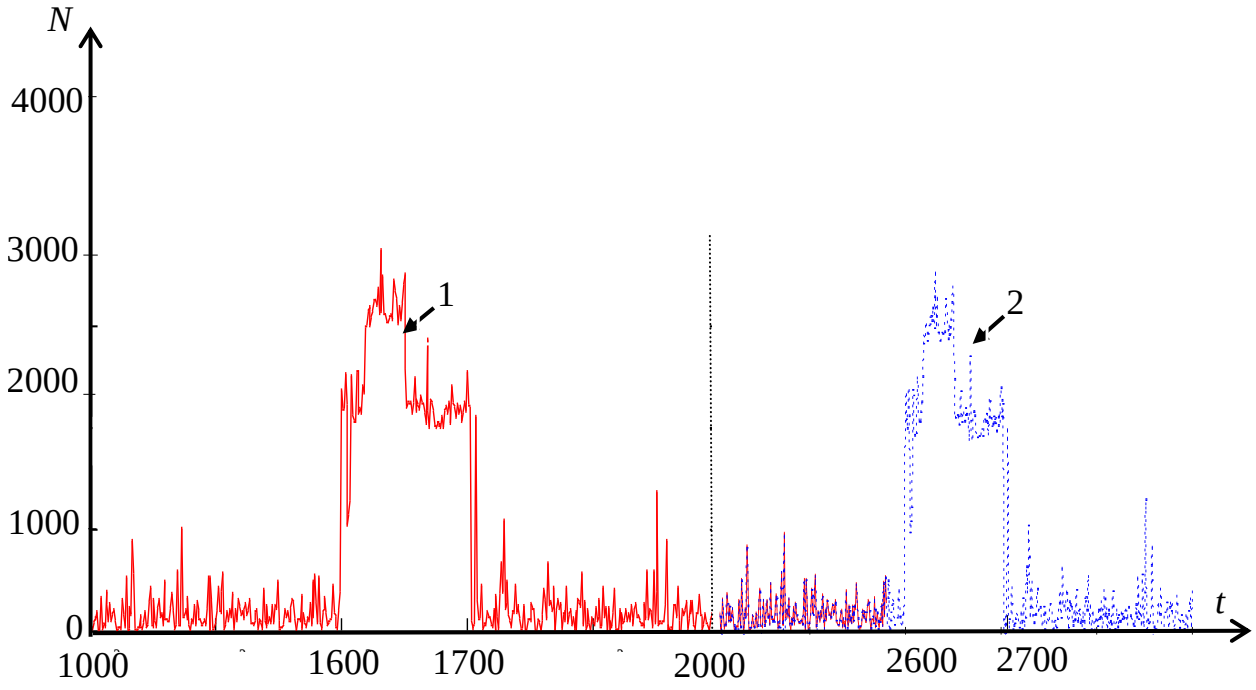


Рисунок 2.4 – Результати екстраполяції інфокомунікаційного трафіку на відрізку [2600;2700] з використанням кубічного сплайну;
1) «сплеск» трафіку; 2) екстраполяція трафіку з використанням лінійного сплайну.

Для знаходження похибки екстраполяції трафіку за допомогою кубічного сплайну використовуємо формулу (2.6) теореми 2. Результати розрахунку зведені у табл. 2.2.

Таблиця 2.2 – Похибка екстраполяції інфокомунікаційного трафіку за допомогою кубічного сплайну

Проміжок	**Числові значення проміжку, мс**	**Значення похибки**
$[x_0; x_1]$	[2600;2601]	1,1
$[x_1; x_2]$	[2601; 2602]	0,05
$[x_2; x_3]$	[2602; 2603]	0,01
$[x_3; x_4]$	[2603; 2604]	5,6
…	…	…
$[x_{10}; x_{11}]$	[2620; 2621]	6,3
$[x_{11}; x_{12}]$	[2621; 2622]	0,1
$[x_{12}; x_{13}]$	[2622; 2623]	4,1
$[x_{13}; x_{14}]$	[2623; 2624]	0,003
…	…	…

З табл. 2.2 видно, що похибка екстраполяції інфокомунікаційного трафіку на відрізку [2600;2700] з використанням кубічного сплайну менше, ніж при екстраполяції трафіку за допомогою лінійних сплайнів. Таким чином, використання кубічних сплайнів дозволяє більш точно визначити «сплески» та отримати прогнозовану «трасу» трафіку.

2.3 Висновки за розділом

Розглянуті методи лінійної та кубічної сплайн-інтерпоялції. Запропонована сплайн-екстраполяція на базі сплайн-функцій, має низку переваг у порівнянні з відомими методами. Вона досить проста у реалізації, має малу похибку, а також може бути використана для визначення та прогнозування інфокомунікаційного трафіку, у тому числі для прогнозування «сплесків» трафіку, зумовлених активністю IoT пристроїв та DDoS кібератак у реальному масштабі часу. Вдалий

вибір виду сплайн-функцій під час сплайн-екстраполяції дозволяє підвищити точність визначення трафіку.

Результати досліджень показали, що похибка екстраполяції інфокомунікаційного трафіку з використанням кубічного сплайну менше, ніж при екстраполяції трафіку за допомогою лінійного сплайну. Це дозволяє зробити висновок, що використання кубічних сплайнів дозволяє більш точно визначити «сплески» та отримати прогнозовану «трасу» трафіку ніж при використанні лінійних сплайнів.

3 ПРОГНОЗУВАННЯ ІНФОКОМУНІКАЦІЙНОГО ТРАФІКУ ЗА ДОПОМОГОЮ КУБІЧНИХ B-СПЛАЙНІВ

3.1 Методи моделювання самоподібного трафіку

Дослідження різних типів інфокомунікаційного трафіку показують, що трафік, який існує в інфокомунікаційних мережах є самоподібним (self-similar) або фрактальним (fractal) за своєю природою. «Самоподібність» є властивістю процесу зберігати свою поведінку та зовнішні ознаки при розгляді в різних масштабах. З цього випливає, що методи моделювання і розрахунку в інфокомунікаційних систем, що використовуються, засновані на використанні пуассонівських потоків, не дають повної і точної картини того, що відбувається в мережі.

Крім того, самоподібний трафік має особливу структуру, що зберігається при багаторазовому масштабуванні. У його реалізації, як правило, є деяка кількість викидів при відносно невеликому середньому рівні трафіку. Це явище погіршує характеристики (збільшує втрати, затримки, джиттер пакетів) під час проходження самоподібного трафіку через вузли інфокомунікаційної мережі. На практиці це проявляється в тому, що пакети, при високій швидкості їх руху по мережі, надходять на вузол не окремо, а цілою пачкою, що може призводити до їх втрат через обмеженість буфера, розрахованого за класичними методиками.

Методи моделювання мережевого трафіку концептуально можна розділити на два класи – аналітичні та імітаційні.

Аналітична модель – це сукупність математичних виразів, що формально описує об'єкт, що моделюється, або процес. Такі моделі зручні щодо теоретичних досліджень, проте, більшість джерел побудова адекватної аналітичної моделі вкрай важко.

Імітаційна модель - це набір алгоритмів, що генерує певну послідовність, яка за своїми характеристиками близька до реальної (експериментально знятої з

чинного об'єкта) послідовності. Як така послідовність, наприклад, може бути мережевий трафік. Використання імітаційних моделей є найчастіше кращим і зручним. У той же час, як правило, імітаційні моделі мають вузьку специфіку, і застосування таких моделей потребує значної роботи для адаптації моделі до нових умов застосування.

Можливі також комбіновані моделі, що поєднують у собі аналітичну та алгоритмічну частини.

Аналіз доступних публікацій з моделювання самоподібного трафіку дозволяє виділити такі моделі.

Фрактальний броунівський рух (Fractional Brown Motion – FBM). В основі моделі FBM лежить випадковий процес, що починається на початку координат з незалежними нескінченно малими гауссівськими приростами. FBM описується аналітично. Також для генерації FBM широко використовуються алгоритми випадкового переміщення середньої точки (RMD-алгоритм) та алгоритми послідовного випадкового додавання (SLA-алгоритм).

Фрактальний гаусівський шум (Fractional Gaussian Noise – FGN). FGN – стаціонарний у широкому значенні стохастичний процес із певним параметрами (середнім значенням, дисперсією, Херстом) та автокореляційною функцією заданого виду. У порівнянні зі звичайним шумом Гауса, FGN має додатковий параметр Херста, який кількісно визначає ступінь фрактального масштабування. Основна труднощі використання FBM і FGN - підбір найкращих значень параметрів для отримання трафіку, що генерується, близького за властивостями до експериментально знятих реалізацій трафіку.

Хаотичні відображення (Chaotic Map – CMAP). Такі моделі є досить поширеними і концептуально простими, вони використовують менше параметрів, ніж FGN і FBM, і їх вибір має більш наочне трактування.

Моделі на основі техніки динамічного моделювання Маркова (Dynamic Markov Modelling – DMM). Ці моделі є автоматами з кінцевим числом станів, що зображуються орграфами або діаграмами станів моделі. У процесі навчання моделі, при отриманні чергового символу вхідного потоку відбувається перехід

моделі в наступний стан і модифікація частотних лічильників, що відповідають ймовірностям переходів. Виходом моделі є набір можливостей появи символів.

Моделі із використанням нечіткої логіки. Побудова нечітких моделей, як правило, заснована на налаштуванні функцій належності за параметрами нечітких множин, що використовуються в правилах, ваги правил і налаштування операцій.

Нейромережні моделі, які дозволяють вирішити завдання апроксимації функцій кількох змінних за навчальною вибіркою шляхом занурення часового ряду в багатомірний простір.

Авторегресійні моделі (Autoregressive Models – AR) широко застосовуються для моделювання та передбачення завдяки властивості тривалої пам'яті самоподібних процесів. У цих моделях поточне значення величини, що генеруються, розраховується як зважена сума N попередніх відліків плюс випадкова змінна. Як різновиди таких моделей використовуються моделі ARMA (процес ковзного середнього), ARIMA (інтегральний процес ковзного середнього) та FARIMA (фрактальний інтегральний процес ковзного середнього). До переваг останньої необхідно віднести можливість гнучкого управління кореляційною структурою (короткочасною та довготривалою залежностями, довільним розподілом).

Фрактальні точкові процеси (Fractal Point Process – FPP) дуже наочні для моделювання самоподібного трафіку. Найпростіший точковий процес представляється на тимчасовій осі ступеневою функцією, що не зменшується, моменти зростання якої є випадковими. Існує багато модифікацій FPP, які досить економічні та обчислювально ефективні.

ON/OFF-моделі. У цих моделях трафік розглядається як комбінація джерел, що його генерують. Кожне джерело має таку структуру. Деякий період часу вони можуть генерувати пакети інформації (так звані ON-періоди), при цьому всередині одного періоду пакети надходять з однаковими інтервалами між ними. Після ON-періоду слідує OFF-період, коли джерело не генерує пакети. Розмір ON- і OFF-періодів є випадковою величиною, яка, повинна мати кінцеве математичне очікування та нескінченну дисперсію.

Фрактальний рух Леві (Fractional Levi Motion – FLM) відноситься до так званих стійких процесів. В основі його моделювання лежать симетричні α-стійкі розподіли, що характеризуються окрім показника Херста, ще й показником Леві. FLM можна розглядати як певне узагальнення FBM та ефективно використовувати для моделювання інтенсивності трафіку або швидкості передачі, що мають теоретично нескінченну дисперсію.

Мультифрактальні моделі (Multifractional – MF) вдало відтворюють трафік, агрегований від кількох істотно відмінних джерел. Мультифрактальність трафіку проявляється у зміні статистичних властивостей реалізації трафіку за зміни масштабу агрегування. Для опису таких властивостей вводяться додаткові масштабна функція та моментний коефіцієнт. В основі моделей MF лежать консервативні бінарні мультиплікативні каскади.

Вейвлет моделі (Wavelet Models) будуються на основі зворотного дискретного вейвлет-перетворення, який полягає у формуванні за допомогою масштабних та вейвлет-коефіцієнтів дискретного часового ряду, використовуючи функції деталізації різного масштабу на основі прототипу смугової вейвлет-функції та низькочастотної скейлінгу. Вейвлет-моделі можуть мати різну кількість параметрів (три і більше) і ефективні для моделювання самоподібного трафіку. Дуже близькими за властивостями до вейвлет-моделей є моделі на основі перетворення сплесків.

Моделі з урахуванням класичних систем масового обслуговування. Як правило, такі моделі вдало описують трафік із пуасонівськими потоками. Однак така модель як M/G/∞ здатна створити приблизно самоподібний трафік шляхом управління поведінкою «хвоста» довільного розподілу обслуговування користувачів, створюючи тим самим довготривалу залежність.

Майже всі розглянуті моделі добре підходять для моделювання самоподібного трафіку даних у інгокомунікаційних мережах з комутацією пакетів. Всі моделі мають такі необхідні для якісного моделювання властивостями, як довготривала залежність, масштабованість, стаціонарність тощо. Однак дослідження експериментально знятих реалізацій трафіку

показують, що характеристики трафіку можуть змінюватися в найширших межах і залежати від великої кількості параметрів та налаштувань реальних мереж, характеристик протоколів, інформації, що передається, і поведінки користувачів. Крім перерахованих вище, виявлено, наприклад, такі характеристики трафіку як наявність короткочасних залежностей, нестаціонарність, мультифрактальність.

Загальним недоліком, моделей інфокомунікаційного трафіку, є їх спрямованість на будь-який конкретний різновид трафіку або мережі і відсутність універсальності. Крім того, застосування їх на практиці призводить до великого обсягу дослідницької роботи, необхідної для адаптації (навчання) моделі до параметрів конфігурації мережі або параметра трафіку. Все це значно ускладнює побудову універсальної моделі, через велику різноманітність, як самих джерел, так і мережевих конфігурацій, що впливають на їхню роботу.

3.2 Метод сплайн-екстраполяції з використанням кубічних В-сплайнів

Використання лінійних та кубічних сплайнів для прогнозування інфокомунікаційного трафіку дозволяє вирішувати як теоретичні, так і практичні питання. Проте у багатьох випадках, у тому числі і при прогнозуванні характеристик самоподібного інфокомунікаційного трафіку, замість кубічних сплайнів краще використовувати В-сплайни. Розглянемо метод прогнозування трафіку за допомогою кубічних В-сплайнів, запропонованих в роботі [30].

Розглянемо самоподібний інфокомунікаційний трафік на відрізку $[a; b]$, який описується функцією $y = f(x)$. Розіб'ємо відрізок $[a; b]$ точками $\Delta: a = x_0 < x_1 < \ldots < x_N = b$, де N – ціле число. Доповнимо множину $\Delta: a = x_0 < x_1 < \ldots < x_N = b$ точками $x_{-3} < x_{-2} < x_{-1} < a$ та $b < x_{N+1} < x_{N+2} < x_{N+3}$. При цьому ці точки обираються довільно. Якщо інфокомунікаційний трафік має періодичну залежність, тоді повинна виконуватись умова $h_{N+1} = h_i$, $i = 0, 1, \ldots, N$.

Побудуємо на інтервалі (x_{i-2}, x_{i+2}) кубічний В-сплайн відмінний від нуля. В-сплайни непарних ступенів зручно нумерувати середнім вузлом їх несучих

інтервалів. Позначимо даний В-сплайн як $B_i(x)$. Визначимо $y_p = B_i(x_p)$, $M_p = B_i''(x_p)$ Кубічний В-сплайн $B_i(x)$ визначається наступним рівнянням [29]:

$$\mu_p M_{p-1} + 2M_p + \lambda_p M_{p+1} = \frac{6}{h_{p-1} + h_p}\left(\frac{y_{p+1} - y_p}{h_p} - \frac{y_p - y_{p-1}}{h_{p-1}}\right), \tag{3.1}$$

де $p = i - 1; i; i + 1$, $\mu_i = \frac{h_{i-1}}{h_{i-1} + h_i}$, $\lambda_i = 1 - \mu_i \lambda_i = 1 - \mu_i$.

Оскільки для $x \notin [x_{i-2}; x_{i+2}]$ $B_i(x) = 0$, тоді:

$$B_i^{(r)}(x_{i-2}) = B_i^{(r)}(x_{i+2}) = 0, \qquad r = 0,\ 1,\ 2., \tag{3.2}$$

У той час як для В-сплайна справедливі співвідношення [31, 32]:

$$B_i(x) = y_i(1-t) + y_{i+1}t - \frac{h_i^2}{6}t(1-t)\left[(2-t)M_i + (1+t)M_{i+1}\right], \tag{3.3}$$

де $x \in [x_i; x_{i+1}]$, $t = \frac{x - x_i}{h_i}$, $h_i = x_{i+1} - x_i$.

Це дозволяє нам записати:

$$B_i' = \frac{y_{i+1} - y_i}{h_i} - \frac{h_i}{6}\left[(2 - 6t + 3t^2)M_i + (1 - 3t^2)M_{i+1}\right], \tag{3.4}$$

$$B_i'' = M_i(1-t) + M_{i+1}t, \tag{3.5}$$

Формула (3.2) з урахуванням (3.3) – (3.5) дозволяє нам записати наступну систему рівнянь:

$$\begin{cases} y_{i-2} = y_{i+2} = 0; \\ M_{i-2} = M_{i+2} = 0; \\ y_{i-1} = \dfrac{1}{6} h_{i-2}^2 M_{i-1}; \\ y_{i+1} = \dfrac{1}{6} h_{i+1}^2 M_{i+1}. \end{cases} \tag{3.6}$$

Видалимо отримані рівняння (3.6) з формули (3.1). Це дозволить нам записати наступну систему рівнянь:

$$\begin{cases} (h_{i-2} + h_{i-1})(h_{i-2} + 2h_{i-1}) M_{i-1} + h_{i-1}^2 M_i = 6y_i; \\ (h_{i-2} + h_{i-1}) M_{i-1} + (h_{i-1} + h_i) M_i + (h_i + h_{i+1}) M_{i+1} = 0; \\ h_i^2 M_i + (h_i + h_{i+1})(2h_i + h_{i+1}) M_{i+1} = 6y_i. \end{cases} \tag{3.7}$$

У результаті ми отримали систему із трьох рівнянь для знаходження чотирьох параметрів: y_i, M_{i-1}, M_i, M_{i+1}. Один із цих параметрів можна задавати довільним шляхом, наприклад:

$$y_i = \frac{h_{i-1}(h_{i-2} + h_{i-1})(2h_i + h_{i+1}) + h_i(h_i + h_{i+1})(h_{i-2} + 2h_{i-1})}{(h_{i-1} + h_i)(h_{i-2} + h_{i-1} + h_i)(h_{i-1} + h_i + h_{i+1})}, \tag{3.8}$$

Із системи рівнянь (3.7) ми знайдемо:

$$\begin{cases} M_{i-1} = \dfrac{6}{(h_{i-2} + h_{i-1})(h_{i-2} + h_{i-1} + h_i)}; \\ M_i = \dfrac{6\left[(h_{i-2} + h_{i-1} + h_i)^{-1} + (h_{i-1} + h_i + h_{i+1})^{-1}\right]}{h_{i-1} + h_i}; \\ M_{i+1} = \dfrac{6}{(h_i + h_{i+1})(h_{i-1} + h_i + h_{i+1})}. \end{cases} \tag{3.9}$$

Формули (3.6), (3.8), (3.9) повністю визначають сплайн $B_i(x)$ на інтервалі $[x_{i-2}; x_{i+2}]$.

Інтерполяційний кубічний сплайн $S(x)$ можна знайти за допомогою представлення B-сплайну:

$$S(x) = \sum_{i=-1}^{N+1} b_i B_i(x).$$

Відповідно до [29] легко знайти похибку екстраполяції самоподібного трафіку. Якість інтерполяційної функції характеризується як $R(x) = S(x) - f(x)$ і залежить від того, які диференціальні властивості має інтерпольована функція $f(x)$.

Розглянемо сплайн, що задовольняє умові:

$$S(f; x_i) = f_i,$$

де $i = 0; 1; \ldots; N$.

Граничні умови цього сплайну визначаються формулою:

$$S'(f; a) = f'(a);$$
$$S'(f; b) = f'(b).$$

Відповідно до [29] для визначення коефіцієнтів b_i отримаємо систему рівнянь:

$$\begin{cases} b_{-1}B'_{-1}(x_0) + b_0 B'_0(x_0) + b_1 B'_1(x_0) = f'_0; \\ b_{i-1}B_{i-1}(x_1) + b_1 B_1(x_1) + b_{i+1}B_{i+1}(x_1) = f_1; \\ b_{N-1}B'_{N-1}(x_N) + b_N B'_N(x_N) + b_{N+1}B'_{N+1}(x_N) = f'_N. \end{cases} \quad (3.10)$$

де $i = 0; 1; \ldots; N$.

Розглянемо періодичний випадок. Тоді рівняння системи рівнянь (3.10), що описують задачу екстраполяції, матимуть вигляд:

$$b_{i-1}B_{i-1}(x_i)+b_iB_i(x_i)+b_{x+1}B_{x+1}(x_i)=f_i\,.$$

де $i = 0; 1; \ldots; N$.

Ми можемо записати у матричному вигляді:

$$Ab=f\,, \tag{3.11}$$

де $b = (b_1; \ldots; b_N)^T$, $f = (f_1; \ldots; f_N)^T$, а T – позначає транспозицію.

Розрахуємо похибку екстраполяції самоподібного трафіку за допомогою (3.11):

$$A(b-f)=f-Af\,. \tag{3.12}$$

Розглянемо простір $C[a; b]$ неперервних на $[a; b]$ функцій з нормою

$$\|f(x)\|_{C[a,b]}=\max_{x\in[a,b]}|f(x)|\,.$$

На сітці $\Delta: a = x_0 < x_1 < \ldots < x_N = b$ ці функції будуть характеризуватися їх коливанням на відрізках $[x_i; x_{i+1}]$

$$\omega_i(f)=\max_{x',x''\in[x_i,x_{i+1}]}|f(x'')-f(x')|\,.$$

та значенням

$$\omega(f)=\max_{0\le i\le N-1}\omega_i(f)\,.$$

Відомо, що незалежною від сітки Δ характеристикою функції є модуль $\omega(f; h)$, який визначається наступним чином

$$\omega_i(f;h) = \max_{\substack{x',x''\in[a,b]\\ |x''-x'|\le h}} |f(x'') - f(x')|, \qquad h \le b-a\ .$$

Якщо позначити $\bar{h} = \max_i h_i$, то отримаємо наступні нерівності:

$$\omega_i(f) \le \omega(f) \le \omega(f;\bar{h})\ .$$

Таким чином:

$$\begin{aligned} \|f - Af\| &= \max_i |f_i - f_{i-1}B_{i-1}(x_i) - f_iB_i(x_i) - f_{i+1}B_{i+1}(x_i)| \le \\ &\le \max_i \{B_{i-1}(x_i)|f_i - f_{i-1}| + B_{i+1}(x_i)|f_i - f_{i+1}|\} \ge \omega(f) \end{aligned}\ .$$

Використовуючи властивості нормалізованого В-сплайну

$$\sum_i B_i(x) = 1\ .$$

та формулу (3.12), отримаємо:

$$\|b - f\| \le \left\|A^{-1}\right\|_{\omega(f)}\ . \qquad (3.13)$$

Звідси

$$\|S(x) - f(x)\| = \left|\sum_{i=-1}^{N+1}[b_i - f(x)]B_i(x)\right| \le \left|\sum_{i=-1}^{N+1}[b_i - f_i]B_i(x)\right| + \left|\sum_{i=-1}^{N+1}[f_i - f(x)]B_i(x)\right|\ .$$

Враховуючи (3.13), отримаємо:

$$\left|\sum_{i=-1}^{N+1}[b_i - f_i]B_i(x)\right| \le \|b - f\| \le \left\|A^{-1}\right\|_{\omega(f)}\ .$$

На доданок, для будь-якого $x \in [x_i; x_{i+1}]$, де $i = 0; 1; \ldots; N$,

$$\left| \sum_{i=-1}^{N+1} [f_i - f(x)] B_i(x) \right| \le \sum_{p=i-1}^{i+2} \left| f_p - f(x) \right| B_p(x) \le 2\omega(f).$$

У кінцевому рахунку, маємо:

$$|S(x) - f(x)| \le \left(2 + \left\|A^{-1}\right\|\right)_{\omega(f)}. \tag{3.14}$$

Введемо $\rho = \frac{\max\limits_i h_i}{\min\limits_i h_i}$. Відповідно до (3.13), матриця A буде необумовленою, якщо $\rho > \frac{(3+\sqrt{5})}{2}$, тоді доцільно використовувати сітку із кроком $\rho < \frac{(3+\sqrt{5})}{2}$.

3.3 Розв'язання задачі екстраполяції самоподібного трафіку методом сплайн-екстраполяції на основі кубічних B-сплайнів

Розглянемо екстраполяцію інфокомунікаційного трафіку за допомогою кубічних B-сплайнів на прикладі. Для цього змоделюємо самоподібний трафік у пакеті Simulink середовища Matlab [33, 34] для системи масового обслуговування (СМО) WB/M/1/K з параметрами:

− інтенсивність пакетів, що потребують обслуговування з визначеною якісю сервісу $\lambda = 125$ пак/с;

− час обслуговування пакетів пакетів $\mu = 150$ пак./с;

− довжина черги пакетів $K = 200$ пак.;

− параметр Херста $H = 0{,}65$;

− параметри розподілу Вейбулла $\alpha \approx 0{,}7$ та $\beta \approx 3{,}46$.

Результати моделювання самоподібного трафіку для заданого часу [3000; 4000] мс, наведено на рисунку 3.1, де n – кількість пакетів, t – час надходження пакету [33, 34].

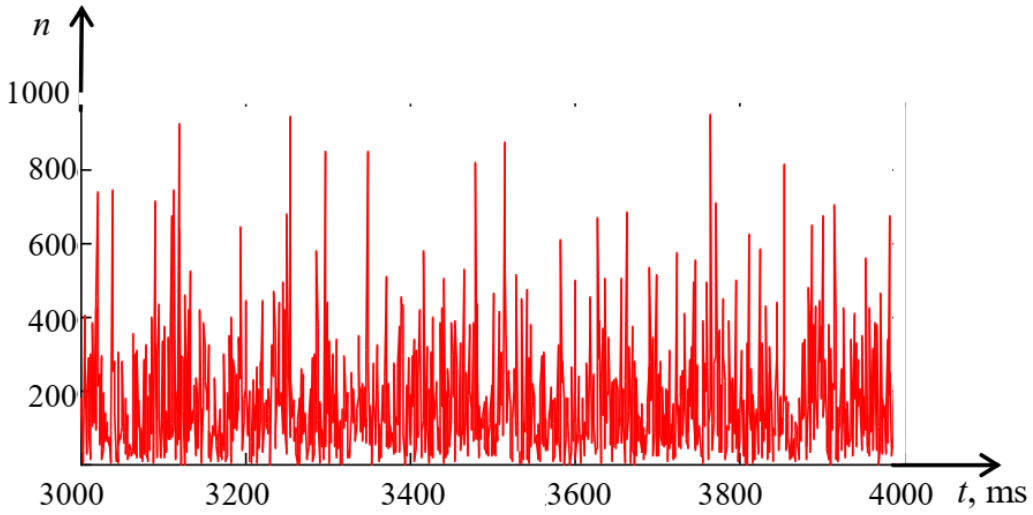


Рисунок 3.1 – Результати моделювання самоподібного трафіку на інтервалі часу [3000; 4000] мс

З рисунку 3.1 видно, що для отриманого самоподібного трафіку для сегмента з часом [3000; 4000] мс, спостерігається великомасштабна інваріантність, наявність «спалахів» запитів і тривалий зв'язок між моментами їх надходження.

Розглянемо екстраполяцію сплайну для змодельованого самоподібного трафіку на інтервалі [3000; 3050] мс, використовуючи кубічний B-сплайн $B_i(x)$ (рис. 3.2).

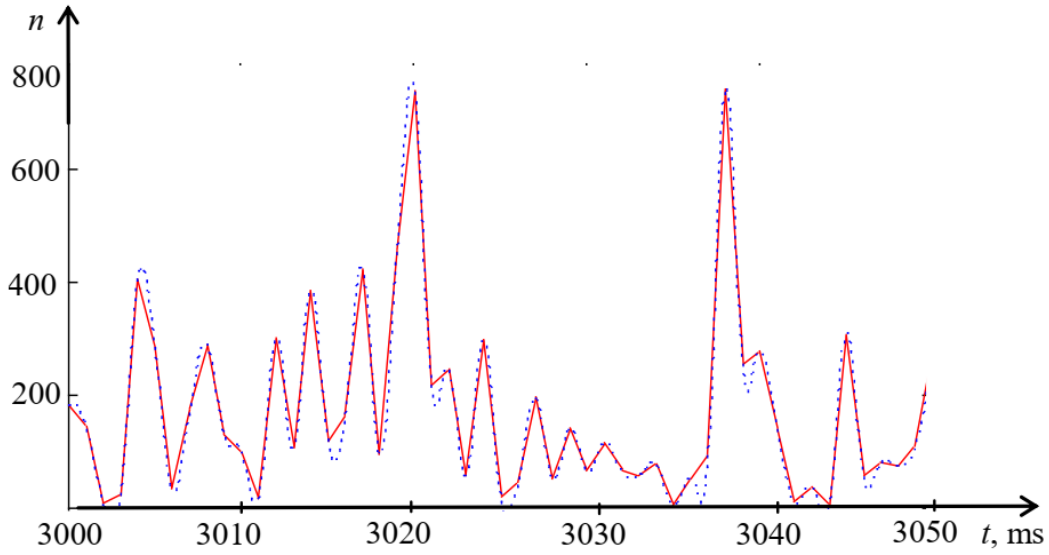


Рисунок 3.2 – Результати екстраполяції самоподібного трафіку на інтервалі [3000; 3050] мс з використанням кубічного B-сплайну

Відповідно до формули (3.14) визначаємо похибку сплайн-екстраполяції для самоподібного трафіку на інтервалі [3000; 3050] мс для заданих часткових інтервалів $[x_i , x_{i+1}]$, $i = 0,1,\ldots, N$ (табл. 3.1).

Таблиця 3.1 – Похибка екстраполяції інфокомунікаційного трафіку за допомогою кубічного сплайну

Проміжок	**Числові значення проміжку, мс**	**Значення похибки**
$[x_0; x_1]$	[3000; 3001]	0,097
$[x_1; x_2]$	[3001; 3002]	0,579
$[x_2; x_3]$	[3002; 3003]	0,337
$[x_3; x_4]$	[3003; 3004]	0,082
…	…	…
$[x_{23}; x_{24}]$	[3023; 3024]	0,121
$[x_{24}; x_{25}]$	[3024; 3025]	0,087
$[x_{25}; x_{26}]$	[3025; 3026]	0,146
…	…	…
$[x_{42}; x_{43}]$	[3042; 3043]	0,546
$[x_{43}; x_{44}]$	[3043; 3044]	0,049
$[x_{44}; x_{45}]$	[3044; 3045]	0,123
…	…	…
$[x_{47}; x_{48}]$	[3047; 3048]	0,912
$[x_{48}; x_{49}]$	[3048; 3049]	0,007
$[x_{49}; x_{50}]$	[3049; 3050]	0,027

За результатами прогнозування трафіку з урахуванням максимальних значень навантажень вузлів мережі можна дати практичні рекомендації щодо перерозподілу трафіку в мережі. Це дозволить збалансувати навантаження на об'єкти мережі та ефективніше використовувати мережеве обладнання.

3.4 Висновки за розділом

Кубічні B-сплайни мають дозволяють адекватно вирішувати практичні задачі прогнозування інфокомунікаційного трафіку. Їх використання дозволяє здійснити подальше спрощення обчислювальних процедур, використовуючи формальні математичні конструкції. При цьому помітно зменшується обсяг інформації, що зберігається в процедурах розрахунку, обсяг цієї інформації

становить $(2N + 5)$ чисел, тоді як для використання звичайних кубічних сплайнів потрібно $3(N + 1)$ чисел, де N – число вузлів інтерполяції.

Використання запропонованого методу екстраполяції на основі кубічних B-сплайнів має низку переваг порівняно з відомими методами: простота реалізації, висока точність прогнозування, можливість достатньо точно екстраполювати пікові спалахи трафіку, що особливо важливо при розв’язанні реальних задач керування трафіком у системах реального часу.

Результати екстраполяції самоподібного трафіку на основі кубічних B-сплайнів дозволять забезпечити необхідний розмір буферних пристроїв, тим самим уникаючи перевантажень мережі та перевищення стандартних значень характеристик QoS.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

1. Проведено аналіз особливостей трафіку в інфокомунікаційних системах. Розглянуто особливості трафіку, що створюється пристроями Інтернету речей та особливості трафіку, що створюється під час кібератак. Показано необхідність використання нових методів прогнозування трафіку.

2. Розглянуто особливості прогнозування інфокомунікаційного трафіку за допомогою лінійних та кубічних сплайнів. Показано, що використання кубічних сплайнів забезпечує більшу точність, порівняно із використанням лінійних сплайнів.

3. Розглянуто особливості прогнозування інфокомунікаційного трафіку за допомогою кубічних B-сплайнів. Показано, що використання кубічних B-сплайнів потребує меншої обчислювальної потужності порівняно із використанням кубічних сплайнів.

4. Результати даної роботи доцільно рекомендувати для практичного застосування у наступних напрямках:

– при проектуванні пристроїв передачі інформації, телекомунікаційної техніки та інших застосунків в яких використовуються технології цифрового передавання інформації;

– під час підготовки фахівців у галузях інформаційних технологій, телекомунікації та радіотехніки, у тому числі і при вивченні методів передавання інформації за допомогою цифрових систем.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. D. Evans, The Internet of Things. How the Next Evolution of the Internet Is Changing Everything, White Paper: Cisco, 2011.

2. 3GPP TR 21.914 V14.0.0, Technical Specification Group Services and System Aspects; Release 14 Description; Summary of Rel-14 Work Items (Release 14), 2018-05. Elektronniy resurs: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3179

3. 3GPP TR 36.888. Study on provision of low-cost Machine-Type Communications (MTC) User Equipment's (UEs) based on LTE (V12.0.0)

4. Sarigiannidis P. Data Traffic Model in Machine to Machine Communications over 5G Network Slicing / P. Sarigiannidis, M. Dighriri, G. Lee, T. Backer, A. S. D. Alfoud// 2016 9th International Conference on Developments in eSystems Engineering (DeSE), Liverpool, UK, 31 Aug.-2 Sept. 2016. – P. 2161-1343. DOI: 10.1109/DeSE.2016.54

5. Bello L.M. Intelligent RACH Access Techniques to Support M2M Traffic in Celluar Networks / Bello L.M., P. Mitchel, D. Grace // IEEE Transactions on Vehicular Technology. ISSN 0018-9545.

6. Бегишев В.О. Стратегии распределения радиоресурсов в гетерогенных сетях с трафиком Narrow-Band IoT / В. О. Бегишев, А. К. Самуйлов, Д. А. Молчанов, К. Е. Самуйлов // Системы и средства информ., 2017, том 27, выпуск 4, 64–79.

7. Begishev V.O. Numerical analysis of the model of distribution of LTE distribution of LTE network resources with narrow-band IoT traffic / V.O. Begishev, E.A. Machnev, E.A. Molchanov, A.K. Samuylov // Proceedings of the II International scientific conference "Convergent cognitive information technologies" (Convergent'2017), Moscow, Russia, November 24-26, 2017.

8. V.V. Krylov and S.S. Samohvalova, Theory of telegraphic and its applications, BXV-Petersburg, 2005.

9. NetFlow Analyzer. Elektronniy resurs: https://www.manageengine.com /ru/netflow/61

10. Стрелковська І.В. Дослідження статистичних характеристик випадкових величин: методичний посібник / І.В. Стрелковська, Л.І. Соколов, О.П. Яковчук. – Одеса: ОНАЗ ім. О.С. Попова, 2004. – 45 с.

11. Strelkovskaya I.V. Self-similar traffic in G/M/1 queue defined by the Weibull distribution/ I.V. Strelkovskaya, T.I. Grygoryeva, I.N. Solovskaya // Radioelectronics and Communications Systems. – 2018. – V. 61, № 3 (2018). – P. 173-180. https://doi.org/10.20535/S0021347018030056

12. Strelkovskaya I.V. Spline-Extrapolation Method in Traffic Forecasting in 5G Networks/ I. Strelkovskaya, I. Solovskaya, A. Makoganiuk // Journal of Telecommunications and Information Technology. – 2019, Vol. 3, pp. 8-16. https://doi.org/10.26636/jtit.2019.134719, ISSN:1509-4553, 1899-8852

13. Про Стратегію кібербезпеки України : Указ Президента № 447/2021 від 14.05.2021

14. Farhadi, H.; AmirHaeri, M.; Khansari, M. Alert correlation and prediction using data mining and HMM. ISeCure 2011, 3, 77–101.

15. Tabia, K.; Leray, P. Bayesian network-based approaches for severe attack prediction and handling IDSs' reliability. In International Conference on Information Processing and Management of Uncertainty in Knowledge-Based Systems; Springer: Berlin/Heidelberg, Germany, 2010; pp. 632–642.

16. Pivarníková, M.; Sokol, P.; Bajtoš, T. Early-Stage Detection of Cyber Attacks. Information 2020, 11, 560. https://doi.org/10.3390/info11120 560.

17. Alghazzawi, D.; Bamasag, O.; Ullah, H.; Asghar, M.Z. Efficient Detection of DDoS Attacks Using a Hybrid Deep Learning Model with Improved Feature Selection. Appl. Sci. 2021, 11, 11634. https://doi.org/10.3390/app112411634

18. Petrik, B.., Dubrovin, V.I. (2021). Detection of DoS attacks in network traffic by wavelet transform. Applied questions of mathematical modelling. 4(1), P. 186-196. https://doi.org/10.32782/KNTU2618-0340/ 2021.4.1.20

19. T. Radivilova, L. Kirichenko, O. Lemeshko and all, "Analysis of anomaly detection and identification methods in 5G traffic," 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2021.

20. Lemeshko O., Yevdokymenko M., Yeremenko M., Kuzminykh I. Cyber Resilience and Fault Tolerance of Artificial Intelligence Systems: EU Standards, Guidelines, and Reports. Proceedings of the Selected Papers on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2020). Kyiv, Ukraine. CEUR, 2020. P. 99-108.

21. O. Lemeshko, O. Yeremenko, A. Shapovalova, A. M. Hailan, M. Yevdokymenko and M. Persikov, "Design and Research of the Model for Secure Traffic Engineering Fast ReRoute under Traffic Policing Approach," 2021 IEEE 16th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), 2021, pp. 23-26, doi: 10.1109/CADSM52681.2021.9385253.

22. O. Lemeshko, O. Yeremenko, M. Yevdokymenko, A. Shapovalova, V. Lemeshko and M. Persikov, "Analysis of Secure Routing Processes Using Traffic Engineering Model," 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2021, pp. 951-955, doi: 10.1109/IDAACS53288.2021.9660980.

23. I. Strelkovskaya, I. Solovskaya and J. Strelkovskaya, «Spline-extrapolation of video traffic of IoT-devices based on various cubic splines,» 2020 International Scientific-Practical Conference Proceedings (PICS&T), 2020, pp. 243-248. https://doi.org/10.1109/PICST51311.2020.9467937

24. I. Strelkovskaya and I. Solovskaya, "Using spline-extrapolation in the research of self-similar traffic characteristics.", Journal of Electrical Engineering, Vol. 70(4), pp. 310-3016, 2019. https://doi.org/10.2478/jee-2019–0061.

25. I.V. Strelkovskaya, I.N. Solovskaya and A.O. Makoganiuk, «Forecasting 5G network multimedia traffic characteristics,» 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer

Engineering (TCSET), 2020, pp. 982 - 987. https://doi.org/10.1109 /TCSET49122. 2020.235585.

26. I. Strelkovskaya, I. Solovskaya, J. Strelkovska, «Spline-approximation and spline-extrapolation methods in telecommunication problems», In: Ilchenko M., Strelkovska I. (eds) Current Trends in Communication and Information Technologies. IPF 2020. Lecture Notes in Networks and Systems, vol. 212. Springer, Chap № 1. https://doi.org/10.1007/978-3-030-76343-5_1.

27. I. Strelkovskaya, I. Solovskaya, A. Makoganiuk and T. Rodionova, «Multimedia Traffic Prediction Based on Wavelet- and Spline-extrapolation,» 2020 8th IEEE International Black Sea Conference on Communications and Networking (Black Sea Com), 2020. https://doi.org/10.1109/BlackSeaCom48709.2020.9234998.

28. P. Dymora, M. Mazurek, «Network Anomaly Detection Based on the Statistical Self-similarity Factor,» Lecture Notes in Electrical Engineering, 324(1). pp. 271-287. https://doi.org/10.1007/978-3-319-11248-0_21

29. Yu.S. Zavyalov, B.I. Kvasov and V.L. Miroshnichenko, Methods of spline functions, 1980.

30. Стрелковська І., Соловська, І., Макоганюк А. Прогнозування характеристик самоподібного руху. Матеріали Третьої міжнародної конференції з питань інформаційних та телекомунікаційних технологій та радіоелектроніки (UkrMiCo´2018). Одеса. − 10-15 вересня 2018. − С. 1-4.

31. Стрелковская И.В. Применение кубических В-сплайнів для селективного синтеза сигналов. Радиотехника, Вып. 142. – 2005. – С. 47-52.

32. Strelkovskaya I.V., Buhan, D.Yu. Comparative analysis of selective signaling functions based on cubic splines and cubic B-splines. Eastern-European Journal of Enterprise Technologies.– Vol. 4/7 (40). – 2009. – Pp. 65-69

33. Стрелковська І.В., Соловська І.Н. Апроксимація самоподібного трафіку за допомогою сплайн-функцій. Матеріали XIII Міжнародної конференції «Сучасні проблеми радіотехніки, телекомунікацій та обчислювальної техніки» (TCET'2016). – Славське, Україна, – 22-26 лютого 2016. С. 132-135. https://doi.org/10.1109/tcset.2016.7451991

34. Strelkovskaya I., Solovskaya I., Severin N., Paskalenko S. Spline approximation based restoration for selfsimilar traffic. Eastern-European Journal of Enterprise Technologies. Vol. 3/4(87), 2017. pp. 45-50. https://doi.org/10.15587/1729-4061.2017.102999

ДОДАТОК А

ПЕРЕЛІК КОПІЙ ДЕМОНСТРАЦІЙНОГО МАТЕРІАЛУ

Слай 1. Титульний слайд

Порівняльний аналіз методів прогнозування трафіку в інфокомунікаційних системах

Виконав: Снігур Назар Орестович
Спеціальність 123 Комп'ютерна інженерія
Керівник: Стрелковська І.В.

Слайд 2. Актуальність роботи

Актуальність роботи

Напрями розвитку інфокомунікаційних мереж – підвищення швидкості передачі даних із збереженням необхідної якості обслуговування

Типи пристроїв Інтернету речей

- Застосунки, що потребують мобільного широкосмугового доступу eMBB
- Застосунки масової міжмашинної взаємодії mMTC
- Застосунки, що потребують надійного з'єднання з низькою затримкою часу URLLC

2

Слайд 3. Основні характеристики роботи

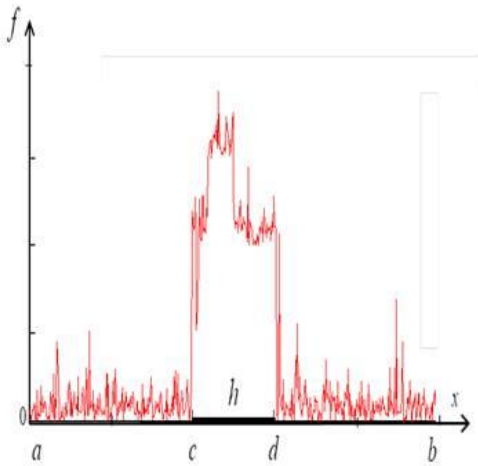
Основні характеристики роботи

- **Об’єкт дослідження** – процеси передачі інформації в інфокомунікаційних системах
- **Предмет дослідження** – математичні моделі для прогнозування трафіку в інфокомунікаційних системах
- **Мета роботи** – визначення методів прогнозування трафіку, придатних для використання в інфокомунікаційних системах
- **Метод дослідження** – методи математичного аналізу, методи теорії зв’язку

3

Слайд 4. Особливості трафіку в сучасних інфокомунікаційних системах

Особливості трафіку в сучасних інфокомунікаційних системах



- Широкий діапазон розміру пакетів
- Широкий діапазон вимог до часу затримки пакетів
- Наявність періодичних та аперіодичних «сплесків»
- Самоподібність

Прогнозування трафіку за класичними методами на основі пуасоновських потоків може призвести до втрат важливої інформації на зниження якості обслуговування

4

Слайд 5. Використання лінійних та кубічних сплайнів

Використання лінійних та кубічних сплайнів

Лінійний сплайн

$$S_1(x) = f_i \frac{x_{i+1} - x}{h_i} + f_{i+1} \frac{x - x_i}{h_i}$$

$$h_i = x_{i+1} - x_i$$

Кубічний сплайн

$$S_3(x) = f_i(1-t)^2(1+2t) + f_{i+1}t^2(3-2t) + \\ + m_i h_i t(1-t)^2 - m_{i+1}h_i t^2(1-t)$$

$$t = \frac{x - x_i}{h_i} \qquad m_i = S'(f; x_i)$$

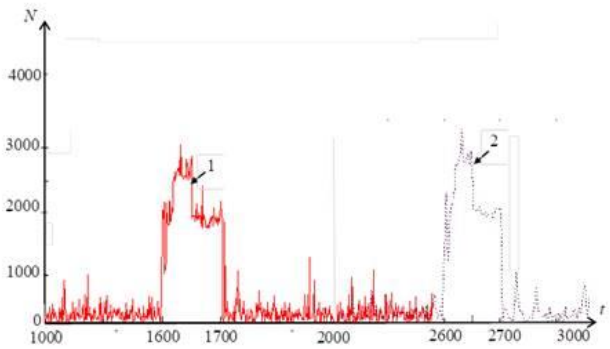
$$S_3(x_i) = f_i \qquad S_3(x_{i+1}) = f_{i+1}$$

5

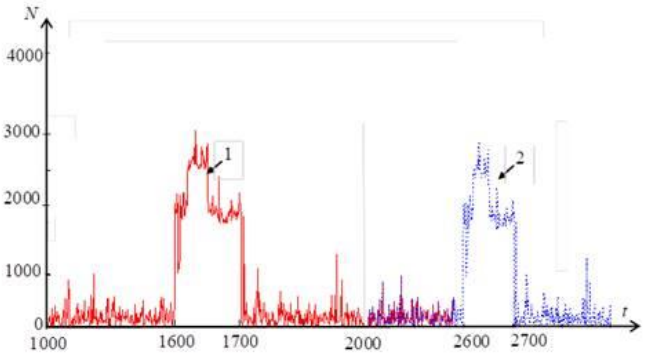
Слайд 6. Результати екстраполяції інфокомунікаційного трафіку за допомогою лінійного та кубічного сплайнів

Результати екстраполяції інфокомунікаційного трафіку за допомогою лінійного та кубічного сплайнів

Лінійний сплайн



Кубічний сплайн



1) «сплеск» трафіку 2) екстраполяція трафіку з використанням лінійного сплайну

6

Слайд 7. Рівняння кубічного В-сплайну

Рівняння кубічного В-сплайну

$$\mu_p M_{p-1} + 2M_p + \lambda_p M_{p+1} = \frac{6}{h_{p-1} + h_p}\left(\frac{y_{p+1} - y_p}{h_p} - \frac{y_p - y_{p-1}}{h_{p-1}}\right)$$

$$p = i-1;\ i;\ i+1 \qquad \mu_i = \frac{h_{i-1}}{h_{i-1} + h_i} \qquad \lambda_i = 1 - \mu_i \lambda_i = 1 - \mu_i$$

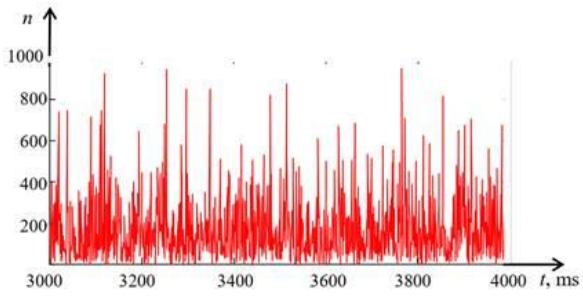
$$y_p = B_i(x_p) \qquad M_p = B_i''(x_p)$$

7

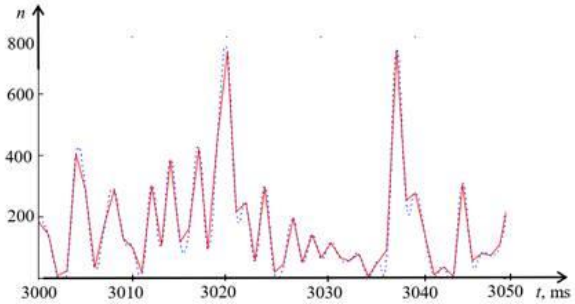
Слайд 8. Результати екстраполяції інфокомунікаційного трафіку за допомогою кубічного В-сплайну

Результати екстраполяції інфокомунікаційного трафіку за допомогою кубічного В-сплайну

Результати моделювання самоподібного трафіку



Результати екстраполяції самоподібного трафіку з використання кубічного В-сплайну



8

Слайд 9. Висновки та рекомендації

Висновки та рекомендації

1. Проведено аналіз особливостей трафіку в інфокомунікаційних системах. Розглянуто особливості трафіку, що створюється пристроями Інтернету речей та особливості трафіку, що створюється під час кібератак. Показано необхідність використання нових методів прогнозування трафіку.

2. Розглянуто особливості прогнозування інфокомунікаційного трафіку за допомогою лінійних та кубічних сплайнів. Показано, що використання кубічних сплайнів забезпечує більшу точність, порівняно із використанням лінійних сплайнів.

3. Розглянуто особливості прогнозування інфокомунікаційного трафіку за допомогою кубічних B-сплайнів. Показано, що використання кубічних B-сплайнів потребує меншої обчислювальної потужності порівняно із використанням кубічних сплайнів.

4. Результати даної роботи доцільно рекомендувати для практичного застосування у наступних напрямках:

– при проектуванні пристроїв передачі інформації, телекомунікаційної техніки та інших застосунків в яких використовуються технології цифрового передавання інформації;

– під час підготовки фахівців у галузях інформаційних технологій, телекомунікації та радіотехніки, у тому числі і при вивченні методів передавання інформації за допомогою цифрових систем.

9

Слайд 10. Заключний

Дякую за увагу!

Снігур Назар Орестович

10

ДОДАТОК Б. ТЕЗИ ДОПОВІДІ НА МІЖНАРОДНІЙ КОНФЕРЕНЦІЇ «ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ» (ОДЕСА, УКРАЇНА, 17-20 ЛИПНЯ 2023 Р.)

УДК 004.946:519.65

Стрелковська І.В., д.т.н., професор, Соловська І.М., к.т.н., доцент,
Снігур Н., магістр 2 року навчання
спеціальності 121 Інженерія програмного забезпечення,
Малюга В., магістр 2 року навчання
спеціальності 122 Комп'ютерні науки
Міжнародний гуманітарний університет
i.strelkovskaya@mgu.edu.ua, i.solovskaya@mgu.edu.ua,
snihurnazar@gmail.com, m4vladaal@gmail.com

ПАРАМЕТРИЧНІ СПЛАЙНИ В 3D-МОДЕЛЮВАННІ

Анотація. Розглянуто 3D-моделювання кривих та поверхонь за допомогою параметричних сплайнів. При інтерполяції кривих та поверхонь використано лінійні параметричні сплайни. Знайдено оцінки похибки інтерполяції при побудові кривих та поверхонь параметричними сплайнами.

Сучасний підхід до моделювання складних двовимірних та тривимірних об'єктів у комп'ютерній графіці (Adobe Photoshop, CorelDraw), Web-дизайні (Figma, Adobe Illustrator, Adobe After Effects) та 3D-моделюванні (Blender, Autodesk 3dsMAX, Maya, LightWave3D, Cinema 4D) базується на використанні кривих та поверхонь, які формуються на базі сплайнів [1].

Сплайнові криві та поверхні дозволяють представляти плавні, гнучкі форми з визначеною кількістю точок, причому криві використовуються для створення форми модельованого об'єкту, а поверхні можуть наближати його тривимірну форму. Особливої уваги заслуговує використання сплайнових кривих та поверхонь у анімації, відеоіграх та інтерактивних додатках, адже створення траєкторії руху об'єктів у часі для створення плавних та природних рухів, процесів деформації у відповідь на дії користувача або зміни у навколишньому середовищі є складним та ресурсновитратним процесом. Проведені авторами дослідження в роботах [1-5] дозволяють стверджувати про перевагу використання сплайнів, адже:

– сплайни просто обчислюються, мають добру збіжність, володіють локальними властивостями,

– сплайни більш стійкі до локальних збурень, тобто поведінка сплайну в околиці точки не позначається на поведінці сплайну в цілому, як, наприклад, це має місце при поліноміальній інтерполяції;

– сплайни мають властивості масштабованості та просто змінюються на окремих ділянках, надають можливості забезпечення необхідної точності.

Сплайнове моделювання передбачає формування ліній або поверхонь за допомогою сплайнів. Набори точок у просторі створюють лінії сплайнів та утворюють каркас розглядаємого об'єкту. В якості сплайн-функцій можуть бути використано різні сплайн-функції (лінійні, квадратичні, квадратичні B-сплайни, кубічні, кубічні B-сплайни і кубічні сплайни Ерміта) [7-8].

Раніше авторами в роботах [2-5] використано дійсні та комплексні сплайни, які дозволили отримати значне підвищення точності апроксимації або екстраполяції при рішенні телекомунікаційних задач. Однак, існує значний клас задач в IT-технологіях, рішення яких може бути отримано за допомогою сплайнів.

В даній роботі для рішення задач моделювання запропоновано використання параметричних сплайнів для побудови кривих та поверхонь, які при виборі визначених сплайн-функцій дозволять отримати результати з більш високою точністю.

Метою даної роботи є моделювання кривих та поверхонь на базі параметричних сплайнів.

Раніше авторами було розв'язано низку телекомунікаційних задач за допомогою дійсних та комплексних сплайнів [1-5]. Задачі моделювання кривих та поверхонь за допомогою сплайн-функцій не було розглянуто. Тому розглянемо інтерполяцію кривих та поверхонь за допомогою лінійних параметричних сплайнів.

Для деяких видів кривих доцільно розглядати їх в параметричному вигляді:

$$\begin{cases} x = x(u); \\ y = y(u), \end{cases} \tag{1}$$

де u – деякий параметр кривої.

Тому доцільно апроксимувати ці криві параметричними сплайнами. При інтерполяції кривої, яку задано параметрично вигляду (3), розіб'ємо проміжок зміни параметру u, таким чином $u_0 < u_1 < \ldots < u_N$. Знайдемо значення функції у точках розбиття u_i, $i = \overline{0, N}$, причому

$$\begin{cases} x_i = x(u_i); \\ y_i = y(u_i). \end{cases} \tag{2}$$

Інтерполяційний параметричний сплайн першого ступеню на проміжку між точками P_i та P_{i+1} заданий співвідношеннями [7]:

$$\begin{cases} S_1(x;s) = (1-t)x_i + tx_{i+1}; \\ S_1(y;s) = (1-t)y_i + ty_{i+1}. \end{cases} \tag{3}$$

де $t = (s - s_i)/l_i$, $l_i = s_{i+1} - s_i$, $i = 0,1,\ldots,N-1$.

Сукупність сплайнів $S(x;u)$ та $S(y;u)$ називається інтерполяційним параметричним сплайном. В залежності від виду функцій $S(x;u)$ та $S(y;u)$ розглядають лінійні параметричні сплайни, квадратичні, кубічні та інші [7]. В цій роботі будемо розглядати лінійні параметричні сплайни.

Розглянемо інтерполяцію кривих лінійними параметричними сплайнами. Нехай на деякій кривій L задано послідовність точок $P_i = (x_i; y_i)$, i = 0, 1, … , N (рис. 1). Введемо параметризацію кривій L:

$$\begin{cases} x = x(s); \\ y = y(s), \end{cases} \tag{4}$$

де s – параметр довжини дуги кривої L.

Вузлу $P_i = P(x_i, y_i)$, де

$$\begin{cases} x_i = x(s_i); \\ y_i = y(s_i), \end{cases}, \; i = \overline{0, N}, \tag{5}$$

відповідає значення параметру s_i.

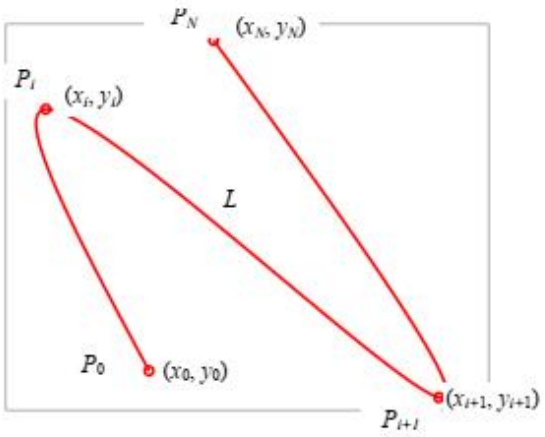


Рисунок 1 – Крива L

Геометрично параметричний сплайн першого ступеню є ламаною, що складається з відрізків прямих, які з'єднують точки P_i, $i = \overline{0,N}$. Згідно (3) отримуємо рівність [7]:

$$\frac{S_1'(y;s)}{S_1'(x;s)} = \frac{y_{i+1} - y_i}{x_{i+1} - x_i}, \quad x_i \neq x_{i+1}, \quad i = 0,1,\ldots,N-1. \tag{6}$$

За допомогою рівності (6) можна наближено розрахувати нахил дотичної до кривої L між точками P_i та P_{i+1}.

Для розрахунку похибки наближення кривої параметричним сплайном використаємо наступні теореми. Для цього позначимо через $R_1(s)$ похибку інтерполяції параметричним сплайном першого ступеню:

$$R_1(\mathrm{S}) = \sqrt{\left|S_1(x;s) - x(s)\right|^2 + \left|S_1(y;s) - y(s)\right|^2}. \tag{7}$$

Теорема 1 [7]. Якщо $x(s),\ y(s) \in \mathrm{W}_\infty^1[s_0, s_N]$, то

$$\left\|\mathrm{R}_1(s)\right\|_\mathrm{C} \le \sqrt{2\bar{l}\,/\,2}, \tag{8}$$

де $\bar{l} = \max_i l_i$, $\mathrm{W}_\infty^1[s_0, s_N]$ – клас функцій, в якому в якості екстремальної функції може бути обраний многочлен другого ступеню.

Теорема 2 [7]. Якщо $x(s),\ y(s) \in \mathrm{CW}_{\Delta,\infty}^1[s_0, s_N]$, то

$$\left\|\mathrm{R}_1(s)\right\|_\mathrm{C} \le \frac{\sqrt{2}}{8}\bar{l}^{\,2}\left\|\mathrm{K}(s)\right\|_\infty, \tag{9}$$

де $\mathrm{K}(s)$ – кривизна кривої L, яка в точці $(x(s), y(s))$ визначається як:

$$\mathrm{K}(s) = \sqrt{\left[x^*(s)\right]^2 + \left[y^*(s)\right]^2},$$

вочевидь, що $\left\|x^*(s)\right\|_\infty \le \left\|\mathrm{K}(s)\right\|_\infty$, $\left\|y^*(s)\right\|_\infty \le \left\|\mathrm{K}(s)\right\|_\infty$.

Побудова параметричного сплайна зводиться до побудови двох сплайнів однієї змінної $S_i(x;s)$ та $S_i(y;s)$.

Розглянемо побудову лінійного параметричного сплайна для заданої кривої *L*. Інтерполяційну криву локального лінійного сплайну виду (3) показано пунктирною лінією на рис. 2.

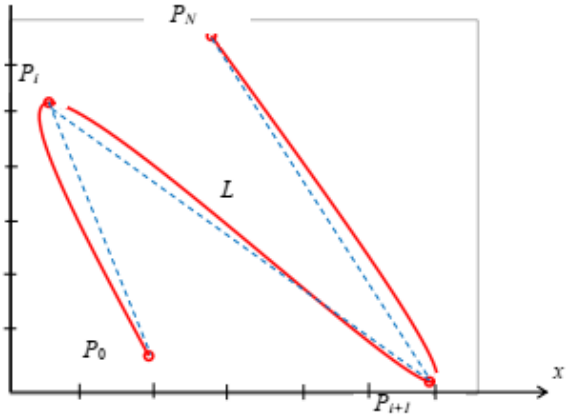


Рисунок 2 – Інтерполяційна крива параметричного лінійного сплайну

Неважко бачити, що така крива має значні похибки до 25 %, зниження яких може бути досягнуто за рахунок зменшення кроку інтерполяції. В цілому, для зменшення похибки можливо використати сплайни вищих порядків, такі як квадратичні або кубічні сплайни, або кубічні В-сплайни.

Висновки

1. Для моделювання кривих та поверхонь запропоновано використання лінійних параметричних сплайнів.
2. Розглянуто принципи побудови інтерполяційних кривих за допомогою лінійних параметричних сплайнів. Знайдено оцінки похибки інтерполяції при побудові кривих та поверхонь параметричними сплайнами.
3. Напрямком подальших досліджень є розгляд кубічних параметричних сплайнів та виконання порівняльного аналізу отриманих результатів для підвищення точності побудови кривих та поверхонь в 3D-моделюванні.

Література

1. Стрелковська І.В., Соловська І.М. Сплайн-апроксимація в 3D-моделюванні VIII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених «Гуманітарний і інноваційний ракурс професійної майстерності: Пошуки молодих вчених»: матеріали конф.,18 листопада 2022 р.: тези доп. – Одеса: МГУ, 2022. – С. 390-394. https://doi.org/ 10.36059/978966-397-266-4/116

2. Стрелковська І.В. Застосування дійсних та комплексних сплайнів в задачах інфокомунікацій [Електроний ресурс] / І.В. Стрелковська, І.М. Соловська, Ю.О. Стрелковська // Проблеми телекомунікацій. – 2021. – № 01 (28). – С. 3-19.

3. Strelkovskaya, I.V., Solovskaya, I.N., Severin, N.V., Paskalenko, S.O. Approximation of self-similar traffic by spline-functions. Modern Problems of Radio Engineering, Telecommunications and Computer Science: proceedings of the XIIIth International Conference (TSET'2016), Slavske, Ukraine, February 23 – 26, 2016. – Lviv: Lviv Polytechnic National University. – P. 132-135.

4. Strelkovskaya, I.V., Solovskaya, I.N., Severin, N.V. Modeling of self-similar traffic. Proceedings of the 4rd International Conference on Applied Innovations in IT (ICAIIT-2016), Vol. 1, Is. 5,

Koethen, Germany, March, 10, 2016.– Anhalt University of Applied Sciences. – P. 61-64. https://doi.org/10.13142/KT10004.23

5. Strelkovskaya, I., Solovskaya, I., Severin, N., Paskalenko, S. Spline approximation based restoration for self-similar traffic. Eastern-European Journal of Enterprise Technologies. (2017). № 3/4 (87). P. 45-50. https://doi.org/10.15587/1729-4061.2017.102999.

6. Strelkovskaya, I., Solovskaya, I., Strelkovska, J. Spline-approximation and spline-extrapolation methods in telecommunication. In: Current Trends in Communication and Information Technologies. IPF 2021. Lecture Notes in Networks and Systems, vol. 212. Springer, Chap № 1. https://doi.org/10.1007/978-3-030-76343-5_1.

7. Ahlberg J.H., Nilson E.N., Walsh J.L. The Theory of Splines and Their Applications, Academic Press, New York, 1967.

8. Larry L. Schumaker Spline Functions: Basic Theory, Cambridge University Press, New York, 2007.