МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО"

АСТРАХАНЦЕВ АНДРІЙ АНАТОЛІЙОВИЧ

УДК 621.391

МОДЕЛІ ТА МЕТОДИ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ТА ЯКОСТІ ПЕРЕДАЧІ ДАНИХ В СИСТЕМАХ МОБІЛЬНОГО ЗВ'ЯЗКУ

Спеціальність: 05.12.02 – Телекомунікаційні системи та мережі

РЕФЕРАТ

дисертації на здобуття наукового ступеня
доктора технічних наук

Київ – 2024

Дисертацією є рукопис.

Робота виконана на кафедрі інформаційних технологій в телекомунікаціях Національного технічного університету України «Київський політехнічний інститут ім. Ігоря Сікорського» Міністерства освіти і науки України.

Науковий консультант: доктор технічних наук, професор
ГЛОБА Лариса Сергіївна, Національний технічний університет України "Київський політехнічний інститут ім. Ігоря Сікорського"

Офіційні опоненти: доктор технічних наук, професор
КИРИК Мар'ян Іванович, Національний університет «Львівська Політехніка», професор кафедри телекомунікацій

доктор технічних наук, професор
ГОЛУБНИЧИЙ Олексій Георгійович, Національний авіаційний університет, професор кафедри телекомунікаційних і радіоелектронних систем

доктор технічних наук, професор
АГЄЄВ Дмитро Володимирович, Харківський Національний університет радіоелектроніки, професор кафедри інфокомунікаційної інженерії

Захист відбудеться «06» грудня 2024 р. о 12.00 годині на засіданні спеціалізованої вченої ради Д26.002.14 у Національному технічному університеті України «Київський політехнічний інститут імені Ігоря Сікорського» за адресою: 03056, м. Київ, пр. Берестейський, 37, корпус 1, ауд. 05.

Захист транслюватиметься на YouTube-каналі Вченої ради КПІ ім. Ігоря Сікорського: https://www.youtube.com/@vchenaradakpi/streams

З дисертацією можна ознайомитись бібліотеці Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», за адресою: 03056, м. Київ, проспект Берестейський, 37, та на сайті Вченої ради Університету за адресою: https://rada.kpi.ua.

Про дату та місце захисту громадськість проінформовано
«06» листопада 2024 р.

в.о. Вченого секретаря
спеціалізованої вченої ради Д 26.002.14
д.т.н., проф. С.Я. Жук

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми.

Впровадження 5G відкриває перед користувачами нові можливості за рахунок появи нових джерел трафіка (таких як Massive IoT, V2V/V2I, eMBMS), істотного підвищення швидкості та зниження затримки. В той же час сама мережа перейшла на новий рівень якості обслуговування за рахунок впровадження таких технологій як розподілені граничні обчислення (MEC), віртуалізація мережних функцій (NFV), мережні зрізи (Network Slicing) та масивний Інтернет речей (mIoT). При цьому поява нових джерел трафіка ускладнює існуючи методи класифікації та обробки трафіка; підвищення швидкості вимагає меншого рівня помилок і, відповідно, більш якісного завадостійкого кодування. Такі технології як NFV та Network Slicing дозволяють ефективніше використовувати ресурси мережі, але трафік який потрапляє до цих сервісів має бути підготовленим. Для вже відомої протягом значного часу технології MEC мережа 5G привносить також нові можливості, пов'язані з розподіленим інтелектом мережі між вузлами, швидкою обробкою трафіка на границі мережі та прямим з'єднанням пристроїв користувача девайс-девайс (D2D), при цьому виникають нові виклики стосовно захищеності та якості передачі даних в системах мобільного зв'язку:

- Активне впровадження нових джерел трафіку призводить до неповного врахування специфіки інформації, що поступає на вхід мережі зв'язку та недостатнього рівня адаптації існуючих методів класифікації та визначення пріоритетів трафіка для забезпечення відповідного рівня якості обслуговування.
- Зростання обсягів трафіку і поява нових типів навантаження (massive IoT, V2V, eMBMS, URLLC) призводять до погіршення ефективності існуючих методів обробки та кластерізації даних, які не були на це розраховані.
- Високі швидкості в 5G досягаються в тому числі застосуванням більш високорівневих алгоритмів модуляції, які є дуже вибагливими до помилок в каналі, що вимагає нових підходів до вдосконалення завадостійкого кодування в мобільних мережах.
- Недостатня адаптація системи захисту інформації до загроз, що виникають під час впровадження новітніх послуг, сервісів та додавання додаткових елементів в мережу. Це потребує вирішення завдання віддаленої автентифікації, в тому числі посилення біометричної автентифікації шляхом поєднання різних біометричних ознак, впровадження методів захисту персональних даних в мобільному пристрої користувача, а також забезпечення шифрування під час розмови для недопущення витоку персональних даних.

Через відсутність методологічної бази та єдиного підходу щодо класифікації трафіка, мережні ресурси використовуються не в повному обсязі, задачі оптимізації вирішені частково або локально, а методи захисту даних частково застарілі, що призводить до погіршення показників захищеності та

якості послуг для кінцевих користувачів. Розроблені в роботі моделі та методи є складовими єдиної архітектури управління ресурсами і захистом даних на рівні провайдера мобільного зв'язку.

Таким чином, створення і наукове обґрунтування комплексної методології управління процесом обслуговування у інформаційно-телекомунікаційній мережі мобільного зв'язку з метою підвищення рівня захищеності та якості передачі й обробки даних є актуальною науково-технічною проблемою.

Зв'язок роботи з науковими програмами, планами, темами.

Дисертація пов'язана з виконанням положень Міністерства Цифрової трансформації України про «Створення тестових центрів розвитку 5G в Україні», «Концепції національної інформаційної політики», «Концепції Національної програми інформатизації», «Концепції розвитку цифрових компетентностей до 2025 року», спільного проекту ІТС НТУУ «КПІ» та університету Анхальт (Hochschule Anhalt) «DigIn.Net 2: Deutsch-ukrainisches Netzwerk digitaler Innovationen-2» (№57602278), а також виконувалась згідно з планами науково-дослідних робіт кафедри інформаційно-телекомунікаційних мереж КПІ ім. Ігоря Сікорського у рамках держбюджетних тем №2117-п «Технологія побудови динамічних реєстрів електронних інформаційних ресурсів та засобів їх ефективної обробки у датацентрах гетерогенної структури» (№ ДР 0118U003522), №2297/19-1 «Гетерогенна мережа збору, передачі та обробки інформації для системи розподіленої генерації» та роботи кафедри ТКС ХНУРЕ № 235-1 «Методи проектування телекомунікаційних мереж NGN та управління їх ресурсами» (№ ДР 0109U000662).

Мета дослідження. Дисертаційна робота присвячена вирішенню важливої науково-технічної проблеми підвищення захищеності та якості передачі й обробки даних в інформаційно-комунікаційних мережах мобільного зв'язку завдяки створенню комплексної методології управління процесом обслуговування у мобільній мережі і сукупності нових моделей та методів передачі, зберігання й обробки даних.

Підвищення завадостійкості, якості передачі та обробки даних в системах мобільного зв'язку досягається за рахунок вдосконалення методів попередньої обробки інформації на боці користувача, методів класифікації, кластеризації та попередньої обробки трафіка у вузлі мережі (на базовій станції), а підвищення захищеності систем мобільного зв'язку – за рахунок вдосконалення методів захисту особистих даних на боці користувача та вдосконалення методів захисту інформації для граничних елементів мережі, які базуються на результатах класифікації трафіку для виявлення загроз.

Задачі дослідження: забезпечення захищеності, якості передачі та обробки даних в 5G мережі мобільного оператора за рахунок нової інтелектуальної методології, яка базується на вперше розроблених моделях та методах завадостійкості, штучного інтелекту для класифікації трафіку, гарантування конфіденційності та спостереженості.

Для досягнення мети дослідження було поставлено та вирішено такі основні задачі:

1) аналіз особливостей передачі трафіка в 5G мережі та наявних загроз, а також визначення основних показників якості та захищеності інформаційно-телекомунікаційної мережі;

2) розробка комплексної методології підвищення захищеності та якості передачі даних в мобільній мережі;

3) визначення набору ознак класифікації трафіку, моделей та методів для адаптивної класифікації трафіка, що підвищує ефективність використання мережних ресурсів під час застосування мережних зрізів (Network Slicing);

4) розробка нового методу обробки даних у вузлі мережі, який підвищує ефективність застосування технології граничних обчислень з множинним доступом (MEC, Mobile Edge Computing);

5) вдосконалення моделей та методів завадостійкого кодування пакетів під час передачі мобільною мережею для зменшення рівня помилок і втрат пакетів;

6) вдосконалення методу формування біометричного шаблону користувача, в тому числі нового методу об'єднання різних біометричних ознак користувача для підвищення рівня конфіденційності та спостереженості;

7) вдосконалення процедури віддаленої автентифікації шляхом застосування методів мережної стеганографії та завадостійкого кодування для підвищення прихованості та завадозахищеності інформації;

8) розробка нового методу взаємної автентифікації користувачів під час дзвінка, що перекриває ряд загроз пов'язаних із шахрайськими схемами підміни користувача;

9) вдосконалення існуючих протоколів обміну повідомленнями під час дзвінка шляхом застосування процедур наскрізного шифрування та перевірки цілісності для підвищення рівня захищеності під час передачі даних в 5G мережі;

10) розробка нових моделей управління приватними даними користувача для забезпечення захищеності даних під час реалізації нових сервісів;

11) перевірка ефективності розробленої методології.

Об'єктом дослідження є процеси обробки і забезпечення захисту інформації в інформаційно-комунікаційних мережах мобільного зв'язку.

Предметом дослідження є моделі, методи та засоби підвищення захищеності та стійкості до атак, а також якості зберігання, обробки та передачі даних в інформаційно-комунікаційних мережах мобільного зв'язку.

Методи дослідження. Основні методи дослідження загальної проблеми – методи теорії масового обслуговування, багатокритеріальної оптимізації, методи математичної статистики, теорії множин і теорії графів, теорії динамічного програмування, теорії ігор і прийняття рішень, методи математичного та імітаційного моделювання, теорії алгоритмів тощо.

Для вибору параметрів та вдосконалення методів класифікації та кластеризації трафіка використовувалася багатокритеріальна оптимізація та методи математичної статистики, при цьому для візуалізації результатів були використані теорія множин і теорія графів. За допомогою теорії динамічного програмування та засобів теорії дослідження операцій було розв’язано ряд оптимізаційних задач пошуку найкращих параметрів класифікації трафіка в мережі. При розробленні методів розподілу трафіка розподілених граничних обчислень МЕС застосовувалися методи теорії масового обслуговування. Для синтезу інтелектуальної системи управління застосовані елементи теорії ігор і теорії прийняття рішень. Під час вдосконалення методів завадостійкого кодування використовувалися методи математичного моделювання. За допомогою імітаційного моделювання проводилася оцінка якості кластеризації трафіка, ефективності роботи інтелектуальної системи та порівняльний аналіз ефективності методів біометричної автентифікації в інформаційно-телекомунікаційній мережі. Методи математичного та імітаційного моделювання використано для розробки методів шифрування та автентифікації користувачів в процесі дзвінка, методів формування біометричного шаблону та об’єднання різних типів біометричних даних. Для оцінки адекватності отриманих теоретичних рішень використано програмні засоби імітаційного моделювання, створені за допомогою Python 3.0.

Наукова новизна отриманих результатів полягає у наступному:

1. Вперше розроблено комплексну методологію обробки даних у вузлі мережі, яка базується на новій онтологічній моделі, використовує інтелектуальну систему управління та відрізняється моделлю попередньої обробки пакетів у вузлі мережі, оптимізацією параметрів класифікації трафіка та модифікованим алгоритмом кластеризації трафіка, що дозволило визначити оптимальний набір ознак класифікації та налаштувати модель нейронної мережі, забезпечуючи високу точність класифікації.

2. Вперше розроблено метод обробки даних у вузлі інфокомунікаційної мережі, який відрізняється наявністю процедур ідентифікації та автентифікації учасників розподілених периферійних обчислень МЕС, виділенням додаткових ресурсів з мобільної мережі, включаючи процедуру підготовки зв'язку точка-точка, а також призначенням обчислювальних вузлів і балансуванням навантаження між ними, за рахунок внесення змін в протокол обміну повідомленнями між базовою станцією та мобільними пристроями, що дозволило економити мережні ресурси, спростити процедуру організації розподілених периферійних обчислень та знизити вартість її розгортання.

3. Вперше розроблено модель коду Raptor та метод формування коду у пристрої користувача, що дозволило на відміну від існуючих моделей та методів одночасно забезпечити підвищення завадостійкості та зменшення ймовірності втрат пакетів.

4. Вперше розроблено методи захисту приватних даних у пристрої користувача, які відрізняються наявністю вдосконалених методів: формування біометричного шаблону, об’єднання різних типів біометричних даних, завадостійкого методу приховування біометричних даних під час передачі, а також забезпечення двобічної автентифікації та наскрізного шифрування під час дзвінка, що дозволило уникнути підміни користувача на іншому боці і отримувати доступ до сервісів лише авторизованому користувачу, підвищити на один рівень надання послуг для забезпечення критеріїв конфіденційності, цілісності та спостереженості.

5. Вперше розроблено моделі для захисту приватних даних у пристрої користувача, які відрізняються: використанням біометричної автентифікації, машинного навчання та розпізнавання зображень для надання користувачу можливості віддаленого управління об’єктами; вдосконаленим методом зберігання приватних даних користувача в захищеному ієрархічному вигляді, що дозволило надати нові можливості під час взаємодії користувача з пристроями mIoT і забезпечити підвищений рівень послуг для критерія конфіденційності при управлінні доступом до персональних даних користувача.

Практичне значення одержаних результатів.

1. Усі теоретичні розробки дисертаційної роботи доведено до конкретних архітектурних рішень, протоколів взаємодії та методів управління сервісами у інформаційно-телекомунікаційних системах нового покоління, які апробовано під час розгортання та обслуговування мереж оператора мобільного зв’язку.

2. Запропонована удосконалена система обробки даних і розподілу ресурсів протестована в лабораторіях компанії Lifecell Ukraine, що дозволило в комплексі з технологіями 5G підвищити швидкість передачі даних до 1.3Гбіт/сек, що підтверджується актом впровадження.

3. Розроблено та впроваджено програмні засоби, які реалізують нові методи захисту приватних даних у мобільних пристроях Samsung, що підтверджується патентами на винахід.

4. Отримані результати використано в навчальному процесі кафедри інформаційних технологій в телекомунікаціях: в лекційних заняттях та компьютерних практикумах з дисциплін «Завадостійке кодування в інформаційно-комунікаційних мережах», «Основи криптографічного захисту інформації» і «Основи побудови захищених банківських інформаційно-телекомунікаційних систем» що підтверджується актом впровадження.

5. Отримані результати впроваджено в навчальному курсі «Основи побудови і захисту мереж 5G» в рамках Міжнародного проекту «PROJECT JEAN MONNET MODULE EU5G4UA», підтверджено авторським свідоцтвом.

Особистий внесок здобувача. Усі наукові результаті, що виносяться на захист дисертації, отримано здобувачем самостійно. Автору належить постановка задач досліджень, теоретичне обґрунтування, їх алгоритмічне забезпечення, експериментальна перевірка нових моделей, методів та

принципів. У спільних публікаціях за темою дисертації автор зробив внесок, який полягає у формалізації ідей, виборі підходів до реалізації, аналізі та узагальненні одержаних результатів.

В роботі [47] автором запропоновано інтелектуальну систему розподілу ресурсів в 5G мережі, при цьому показники ефективності та завадостійкості автором визначено в роботі [5].

В роботах [23,25,48,50] автором визначено оптимальний набір ознак для класифікації трафіка, оцінено ефективність застосування методів машинного навчання для вирішення задач класифікації трафіка та запропоновано рекомендації щодо їх використання і значень гіперпараметрів. Робота [21] висвітлює вдосконалений метод кластеризації трафіка.

В роботах [8-9] автором запропоновано вдосконалені методи формування коду Raptor, формування коду LDPC, як одного з елементів коду Raptor, а також вдосконалення методу декодування коду Raptor.

Новий метод обробки даних у вузлі мережі, який підвищує якість застосування технології граничних обчислень з множинним доступом представлено в роботі [3].

Новий метод зберігання приватних даних користувача в захищеному ієрархічному вигляді, який надає нові можливості під час взаємодії користувача з пристроями mIoT запропоновано в статті [49] та патентах [35,39]. Новий метод формування біометричного шаблону та спосіб об'єднання різних типів біометричних даних описано в роботах [14,17] і патенті [40].

В роботах [20,22] автором розроблено методи підвищення завадостійкості біометричних шаблонів до зовнішніх впливів під час передачі мобільними мережами. В [1,24,44-46,51] автором запропоновано стеганографічні методи прихованої передачі біометричних даних із забезпеченням підвищеної стійкості до атак та завад в каналах зв'язку.

Запропоновані автором завадостійкі методи прихованої передачі приватної, в тому числі біометричної інформації, стійкі до дії завад в каналах зв'язку наведено в [6,7,11-16,18,29-31,43]. Методику оцінювання важливості характеристик стеганографічних алгоритмів наведено в [10].

Запропоновані вдосконалення протоколів обміну повідомленнями під час дзвінка для підвищення рівня захищеності 5G мережі наведено в [2,42].

Запропоновані нові методи захисту приватних даних на боці пристрою користувача, які відрізняються використанням біометричної автентифікації, машинного навчання та розпізнавання зображень для надання користувачу можливості віддаленого управління об'єктами, наведено в патентах [36,37].

Запропоновані методи у поєднанні з застосуванням мережних зрізів, які дозволять зменшити затримку передачі і покращити ефективність 5G мережі в цілому, знайшли відображення у авторському свідоцтві [41].

Апробація результатів дисертації. Основні положення і результати дисертаційної роботи були представлені, повідомлені й одержали схвалення на

27 науково-технічних конференціях: 1-а Міжнародна конференція «Безпека та захист інформації в інформаційних та телекомунікаційних системах» (м. Харків, ХНЕУ, 2008), 13-й,14-й,15-й,19-й,21-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті» (м. Харків, ХНУРЕ, 2009-2011,2015,2017), Інфокомунікації – сучасність та майбутнє: 1-й міжнар. наук.-пр. конф. молодих вчених (м. Одеса, ОНАЗ, 2011), International Conference on Modern Problem of Radio Engineering, Telecommunications and Computer Science TCSET'2012 (м. Львів-Славсько, 2012), 9-я Міжнародна молодіжна науково-технічна конференція «Сучасні проблеми радіотехніки і телекомунікацій РТ-2013» (м. Севастополь, СевНТУ, 2013), 23rd International Crimean Conference «Microwave&Telecommunication Technology» (м. Севастополь, СевНТУ, 2013), International Scientific-Practical Conference Problems of Infocommunications Science and Technology "PICS&T" (м. Харків, 2014,2015,2019), Міжнародна науково-практична конференція «Проблеми і перспективи розвитку IT-індустрії» (м. Харків, ХНЕУ, 2017), IEEE 9th International Conference on Dependable Systems, Services and Technologies "DESSERT" (м. Харків, 2018), 73 науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів (м. Одеса, ОНАЗ, 2018), Workshop on Cybersecurity Providing in Information and Telecommunication Systems "CPITS" (м. Київ, 2021), International Conference on Information and Digital Technologies "IDT" (Zilina, Slovakia, 2021), 17-а Міжнародна науково-технічна конференція "Перспективи телекомунікацій" (м. Київ, НТУ КПІ, 2023), IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics (м. Київ, НТУ КПІ, 2023), International Scientific and Technical seminar Critical Computer Technologies and Systems (CriCTecS 2024), IEEE International Black Sea Conference on Communications and Networking (Tbilisi, Georgia, 2024).

Публікації. Основні положення дисертації, які в достатній мірі висвітлюють результати роботи, що виносяться на захист, опубліковано у 76 наукових працях, у тому числі у 3 навчальних посібниках (зокрема 1 з грифом МОНУ), 31 публікаціях у наукових фахових виданнях (3 статті у виданнях категорії «А», 3 статті у виданнях іноземних держав, 25 статей у науково-фахових виданнях України), 6 патентів на корисну модель, 1 авторське свідоцтво на твір, 35 тезах доповідей в збірниках матеріалів конференцій (в тому числі 10, які включені до міжнародних наукометричних баз).

Структура і обсяг дисертації. Дисертація складається з анотацій, вступу, 5 розділів основного змісту, висновків, списку використаних джерел. Загальний обсяг роботи становить 377 сторінок друкарського тексту, в тому числі список літератури із 294 найменувань, робота містить ілюстрації та таблиці.

ОСНОВНИЙ ЗМІСТ ДИСЕРТАЦІЇ

У **вступі** обґрунтовується актуальність теми дисертаційної роботи. Визначено мету роботи, основні задачі та методи досліджень. Сформульовано наукову новизну і практичне значення отриманих результатів.

У **першому розділі** *проаналізовано особливості передачі трафіка в 5G мережі та наявні загрози, а також визначено основні показники якості та захищеності інформаційно-телекомунікаційної мережі*. Проаналізовано особливості функціонування мобільної мережі на основі стандарту 5G-NR, визначено її складові, основні технологічні особливості, показники захищеності даних та якості обслуговування користувачів, фактори впливу на них.

Структуру мобільної мережі на основі стандарту 5G-NR умовно розділяють на декілька частин (рис. 1):

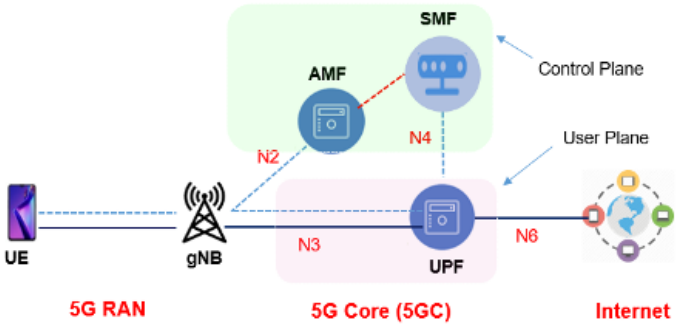


Рис. 1. Узагальнена архітектура мережі 5G

- Обладнання користувача (UE), наприклад смартфони, підключаються через мережу радіодоступу 5G до ядра 5G і далі до мереж передачі даних.
- 5G RAN – канал зв'язку, радіомережа, яка поєднує користувацьке обладнання з базовими станціями;
- 5G Core – ядро мережі, яке відповідає за всі функції та взаємодії в мережі 5G, включаючи автентифікацію, безпеку, управління сеансами та агрегацію трафіку з кінцевих пристроїв.

В наступних розділах запропоновано методи по вдосконаленню захищеності та якості передачі даних у обладнанні користувача, базовій станції (gNB) і ядрі мережі. Розглянемо ключові технологічні особливості мереж 5G-NR, які впливають на перелік та якість послуг, що надаються:

Віртуалізація мережних функцій (*NFV*) – відокремлює програмне забезпечення від апаратного, замінюючи різні мережеві функції. Це забезпечує набагато більшу гнучкість у розгортанні мережі. Обслуговування також значно спрощується, оскільки можна легко створити тимчасову мережну функцію.

Граничні обчислення з множинним доступом (*MEC*) – прикладні програмні компоненти, такі як віртуальна реальність, розумні фабрики або автономне водіння, дуже вимогливі до часу відгуку передачі даних. Щоб скоротити цей час деякі "локальні реплікації" головного сервера виносяться ближче до

кінцевого користувача. Функція MEC дозволяє частину розрахунків виконати безпосередньо на границі мережі, в тому числі за допомогою обладнання користувача і забезпечити низьку затримку, високу пропускну здатність й обробку інформації у режимі реального часу. В тому числі це дозволяє суттєво розвантажити мережу передачі даних.

Масивний Інтернет речей (mIoT). MIoT обслуговує мільярди недорогих, ультраенергоефективних підключених пристроїв у віддалених місцях, а також хмарні сервіси, які не потребують частого зв'язку або зв'язку в реальному часі. Забезпечує збір даних від сенсорів та керування ними.

Нарізка мережі (Network Slicing) є ключовим компонентом для реалізації повного потенціалу архітектури 5G. Нарізка мережі дозволяє операторам ефективно керувати різними сервісами з різними вимогами до пропускної здатності, затримки та доступності, розподіляючи мережеві ресурси між кількома користувачами. Крім того, нарізка мережі необхідна для підтримки граничних обчислень та обслуговування mIoT, де кількість користувачів може бути надзвичайно великою, а рівні необхідних сервісів – різними.

Згідно «Методики вимірювань параметрів якості послуг рухомого (мобільного) зв'язку», якість телекомунікаційної послуги – це сукупність показників, які характеризують споживчі властивості телекомунікаційної послуги та визначають її здатність задовольнити заявлені, встановлені і замовлені потреби споживача послуги.

Розглянемо більш детально показники якості мобільної мережі, згідно вказаної методики, які мають бути вдосконаленими в даній роботі.

1. *Середня швидкість передавання даних* ($V_{шв}$) визначається як відношення розміру отриманих даних до часового інтервалу від початку передачі даних до кінця. Середню швидкість передавання даних у Мбіт/с обчислюють за формулою:

$$V_{\text{шв } HTTP} = \frac{W_{\text{роз дан}}}{T_{\text{ПД зав}} - T_{\text{ПД поч}}}, \quad (1)$$

Де $W_{\text{роз дан}}$ – розмір даних користувача, Мбіт;
$T_{\text{ПД зав}}$ – час завершення передачі даних, с;
$T_{\text{ПД поч}}$ – час початку передачі даних, с.

2. *Час затримки між відправленням та прийманням пакетів* (T_{ping}) визначається як половина часу в мілісекундах між відправкою запиту та отриманням відгуку. Середній час затримки між пакетами T_{ping} розраховується за формулою:

$$T_{ping} = \frac{\sum_{i=0..n} T_i}{n} \quad (2)$$

де T_i – половина часу затримки пакета з номером i;

n – кількість пакетів у вимірювальному циклі.

3. *Варіація затримки пакетів* (тремтіння, *J*) визначає максимальне відхилення часу затримки передачі (прийому) пакетів відносно середнього значення часу затримки передачі (прийому) пакетів впродовж вимірювання. Розраховується за формулою:

$$J = \max_n(D_{сер} - d_i) \quad (3)$$

де $D_{сер}$ – середня затримка передачі пакетів;

d_i – затримка окремого пакета.

4. *Втрата пакетів* (відсоток втрати пакетів, $Ping_{drop\_ratio}$) визначається як кількість неотриманих відгуків після відправлення запитів. Відсоток втрати пакетів розраховується за формулою:

$$Ping_{drop\_ratio} = Ping_{lost} / Ping_{total} \times 100\% \quad (4)$$

де $Ping_{lost}$ – кількість неотриманих відгуків;

$Ping_{total}$ – загальна кількість відправлених запитів.

Оскільки вказані показники нерозривно пов’язані з телекомунікаційними послугами, що надаються, то потрібно оцінювати ступінь їх впливу на різні програмні середовища та послуги, що обслуговуються 5G мережею, а враховуючи, що 5G мережа орієнтована в першу чергу на пакетний трафік, то наведемо ступінь важливості вказаних показників саме для пакетних сервісів 5G мережі (табл. 1).

Таблиця 1 – Вплив параметрів якості на продуктивність пакетних додатків

Додаток	Оцінка ефективності роботи
Перегляд web-сторінок (*Web-browsing*)	Показник продуктивності – швидкість оновлення сторінки після запиту. Обмеження на час затримки (до декількох секунд).
Пріоритетні транзакційні послуги (*High-priority services*)	Безперебійна транзакція має обмеження на час затримки – декількох секунд.
Управління (*Command/control*)	Дуже жорсткі обмеження на затримку (долі секунди), нульовий рівень втрат пакетів.
Нерухомі зображення (*Still images*)	Рекомендація рівень втрат пакетів близький до нуля.
Інтерактивні ігри (*Interactive games*)	Обмеження на час затримки (долі секунди).
Telnet	Обмеження на час затримки (долі секунди).
Електронна пошта E-mail (*server access*)	Обмеження на час затримки (до декількох секунд).
Фонові додатки (*Background apps*)	Рекомендація рівень втрат пакетів близький до нуля. Рекомендація – обмеження максимальної затримки.

Поєднуючи результати, наведені в табл. 1 з вищенаведеними характеристиками, можна побачити, що для якісної передачі даних необхідно

забезпечення високої швидкості передачі даних, низького рівня затримки обробки та передачі даних і низького рівня помилок та втрат пакетів.

Зменшення рівня помилок і втрат пакетів під час їх доставки можна досягти вдосконаленням методів завадостійкого кодування.

Зменшення затримки під час обробки та передачі можна досягти вдосконаленням процедур класифікації трафіка, кластеризації та інтелектуальної обробки на основі заздалегідь заданих правил.

Підвищення швидкості передачі пакетів може бути досягнуто застосуванням інтелектуальної системи управління зі зворотним зв’язком для контролю параметрів каналу зв’язку і вибору оптимальних за певних умов параметрів завадостійкого коду.

Мережа мобільного зв’язку сьогодні являє собою складну систему, яка забезпечує не лише доступ до різноманітних сервісів та гарантує якість обслуговування, але й має забезпечувати захищеність даних.

Відповідно до документу НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу», захищеність в інформаційно-телекомунікаційній системі (ІТС) може розглядатися як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз і може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного.

Функціональні критерії оцінки захищеності розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів.

1) Конфіденційність. Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності. Конфіденційність забезпечується послугами: довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні.

2) Цілісність. Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності. Цілісність забезпечується такими послугами: довірча цілісність, адміністративна цілісність, відкат, цілісність при обміні.

3) Доступність. Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності. Доступність може забезпечуватися наступними послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

4) Спостереженість. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет послуг

спостереженості і керованості. Спостереженість забезпечується послугами: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність засобів захисту, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача.

Також НД ТЗІ 2.5-004-99 декларує, що реалізація біометричної автентифікації дозволяє забезпечувати значно сильнішу автентифікацію, ніж парольна автентифікація та автентифікація за допомогою фізичних об’єктів.

Останнім часом багато робіт присвячуються вдосконаленню якості послуг, що надаються мережею і захищеності даних користувачів. При цьому, зазвичай вдосконалюються окремі елементи і недостатньо уваги приділяється системі в цілому.

В **розділі 2** запропоновано комплексну методологію забезпечення якості передачі та захищеності даних у системі мобільного зв’язку, яка базується на удосконаленій структурі мережі мобільного зв’язку 5G (рис. 2) і онтологічній моделі. Запропонована структура забезпечує покращення наведених в розділі 1 показників якості (рівень помилок і втрат пакетів, швидкість передачі інформації, затримка передачі й обробки інформації), показників захищеності (конфіденційність, цілісність, доступність та спостереженість). Для підвищення значень показників якості передачі даних запропоновано поетапне впровадження у вузлі мережі (gNB, рис. 1), наступних модифікацій (рис. 2):

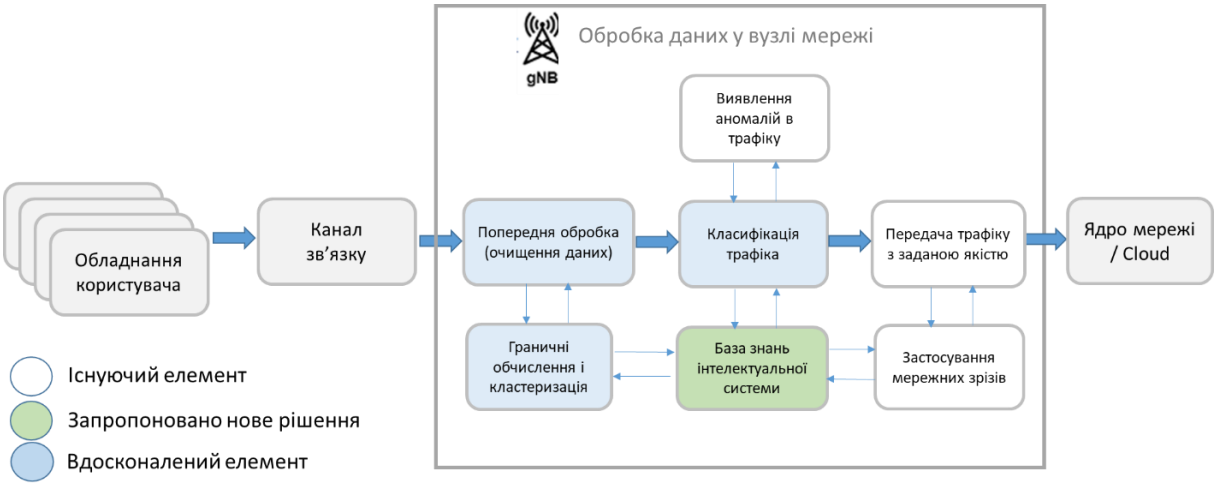


Рис. 2. Вдосконалення обробки даних у вузлі мобільної мережі

1) вдосконалення методів попередньої обробки даних у вузлах мережі для підвищення точності класифікації і обробки трафіка та зменшення затримки на обробку даних;

2) впровадження новітніх адаптивних методів класифікації трафіка для підвищення ефективності використання мережних ресурсів під час застосування мережних зрізів (Network Slicing);

3) впровадження нових методів розподілу трафіка на граничних елементах мережі для підвищення якості застосування технології граничних обчислень з множинним доступом (Mobile Edge Computing);

4) вдосконалення методів завадостійкого кодування пакетів під час їх передачі мобільною мережею для зменшення рівня помилок і втрат пакетів.

При цьому, вдосконалення методів завадостійкого кодування пакетів пропонується до реалізації у модемній частині обладнання користувача (рис. 3).

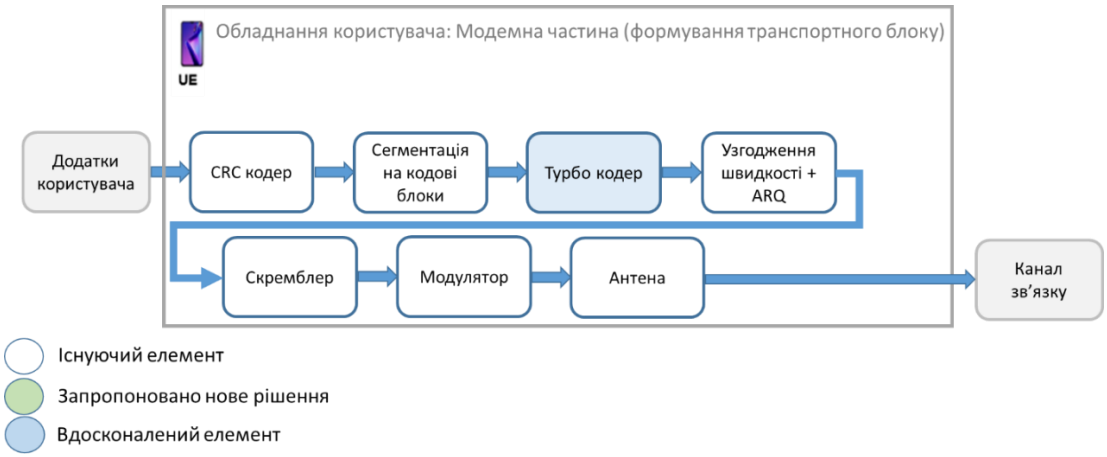


Рис. 3. Вдосконалення обробки даних в модемній частини обладнання користувача

Рис. 4. Вдосконалення показників захищеності через зміни в програмній частині обладнання користувача

Для вдосконалення показників захищеності, комплексна методологія пропонує поетапне впровадження у обладнанні користувача (UE, рис. 1), наступних модифікацій (рис. 4):

5) вдосконалення методу формування біометричного шаблону користувача, в тому числі нового методу об'єднання різних біометричних ознак користувача;

6) застосування методів мережної стеганографії та завадостійкого кодування для підвищення прихованості та завадозахищеності інформації під час проходження процедури віддаленої автентифікації;

7) впровадження нового методу взаємної автентифікації користувачів під час дзвінка, що перекриває ряд загроз пов'язаних із шахрайськими схемами підміни користувача;

8) впровадження нового методу наскрізного шифрування під час дзвінка для підвищення рівня показника конфіденційності;

9) впровадження нових методів управління приватними даними користувача для забезпечення захищеності під час реалізації нових сервісів.

Відповідно до запропонованої комплексної методології підвищення захищеності та якості передачі даних в мобільній мережі (рис. 2-4), в наступних розділах описуються наведені вище кроки підвищення показників елементів системи. Так, розділ 3 дисертаційної роботи присвячений вдосконаленню обробки даних у вузлі мобільної мережі (рис. 2). Розділ 4 висвітлює підходи до вдосконалення моделей та методів завадостійкого кодування (рис. 3), а розділ 5 присвячений підвищенню показників захищеності даних користувача та інформаційно-комунікаційної системи в цілому (рис. 4).

2) Вдосконалення методів попередньої обробки даних у вузлах мережі, що підвищує точність класифікації та обробки трафіка, а також зменшує затримку на обробку даних.

Наразі актуальним є завдання розробки методології, яка б враховувала взаємозв'язок між якістю обслуговування кінцевих користувачів та процесами розподілу обчислювальних ресурсів між віртуальними сутностями з урахуванням енергоефективності та продуктивності обчислювальних процесів.

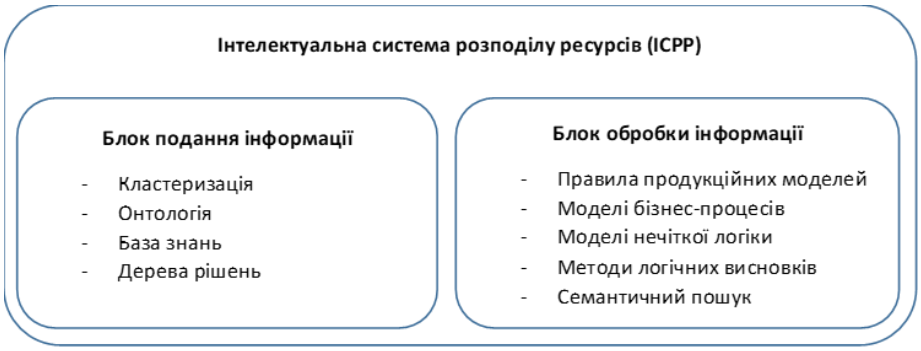


Рис. 5. Запропонована модель інтелектуальної системи розподілу ресурсів

Вказане завдання вирішується шляхом створення інтелектуальної системи розподілу ресурсів (ІСРР) (рис. 5), яка:

• дозволяє координувати якість зв'язку (через підготовку модифікованої системи розподілу ресурсів);

• використовує онтологічну модель та систему нечіткої логіки для покращення обробки даних в модифікованій системі розподілу ресурсів;

• забезпечує високий рівень безпеки (за допомогою врахування та впровадження підходів безпеки 5G).

Кожен елемент набору інтелектуальних моделей та методів, показаний на рис. 5, виконує певну функцію, а саме:

1. Кластеризація використовується під час розподілу ресурсів (в тому числі під час MEC), що забезпечує високий рівень обчислювальної продуктивності та дотримання вимог до якості обслуговування.

2.Онтологія інтегрує всі наявні компоненти інформаційно-телекомунікаційної системи та інтелектуальні компоненти управління процесами надання телекомунікаційних послуг і дозволяє динамічно обирати сценарії обслуговування в мережах 5G.

3. База знань виступає центральним репозиторієм і зберігає інформацію, якою оперує ICPP, експертні правила, метаописи послуг та бізнес-процесів.

4. Дерева рішень реалізують механізми інтелектуального планування та прогнозування потреб користувачів відповідно до різних періодів часу.

5. Правила дозволяють реалізувати механізми підтримки прийняття рішень (на основі експертних правил) щодо визначення обсягів вхідного навантаження для використання ресурсів підсистем обслуговування, які дозволять забезпечити обслуговування із заданими показниками якості.

6. Моделі бізнес-процесів реалізують формування послідовності надання послуг при динамічному обранні сценаріїв обслуговування абонентів в мережах 5G, а також підвищують якість послуг за рахунок автоматизованого розрахунку оцінки якості їх надання.

7. Методи нечіткої логіки покладено в основу алгоритму оцінки поточного стану надання послуг оператором зв'язку за допомогою інтегрального показника якості надання послуг.

8. Семантичний пошук забезпечує пошук великих обсягів розподіленої інформації, отриманих від mIoT, на основі онтології, бази знань та дерев рішень.

При цьому, блок обробки інформації (рис. 5) готує отриману з мережі інформацію (наприклад, пакети, які підлягають класифікації або трафік, що має бути розподілений по вузлах граничних обчислень) до класифікації трафіка або його кластеризації. Сутність такої підготовки полягає в попередній обробці, побудові правил нечіткої логіки, видаленні дублікатів і застосуванні інших процедур, що можуть підвищити ефективність класифікації або розподілу трафіку.

В **розділі 3** для зменшення сумарної затримки передачі трафіка було вдосконалено методи обробки пакетів у вузлі мережі за рахунок раціонального вибору параметрів та методів класифікації трафіка, оптимізації кількості ознак, які використовують під час класифікації, а також розроблено новий метод обробки даних у вузлі мережі, який підвищує ефективність застосування технології граничних обчислень з множинним доступом. Запропоновані методи

у поєднанні з застосуванням мережних зрізів дозволяють зменшити затримку передачі трафіка і покращити ефективність 5G мережі в цілому, що знайшло відображення у авторському свідоцтві [30].

3) Визначення набору ознак, методів та їх параметрів для адаптивних методів класифікації трафіка, що підвищує ефективність використання мережних ресурсів під час застосування мережних зрізів (Network Slicing).

Під час обробки трафіку швидкість роботи класифікатора визначає швидкість і ефективність роботи мережі в цілому (виражену в швидкості обробки пакетів), а також можливий рівень втрат пакетів. Відповідно, завдання забезпечення максимальної продуктивності класифікатора є актуальним. Його продуктивність напряму залежить від кількості ознак, що обробляються та алгоритму класифікації.

На першому етапі застосування методів класифікації трафіка засобами ICPP виконано підготовку датасету: відфільтровано додатки, які не мали достатнього рівня репрезентації в датасетах (менше 250 записів), а також неповні записи і дублікати. Для новітніх алгоритмів класифікації трафіка на основі методів машинного навчання, таких як RF, ANN, KNN, AdaBoost, SVM досліджено ефективність класифікації за допомогою підготовленого набору програм на мові Python 3.0, через оцінку таких характеристик як точність (accuracy), чіткість (precision) та інші метрики.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}, \quad (5)$$

На основі попередньо підготовленого, збалансованого набору даних визначено найкращі параметри моделі та точність класифікації для кожного з алгоритмів (табл. 2) при навчанні й тестуванні на тому ж самому датасеті.

Таблиця 2. Порівняльний аналіз точності алгоритмів класифікації

Алгоритм	Accuracy	Precision	F1-score
ANN	0.991	0.992	0.991
KNN	0.933	0.933	0.933
RF	0.993	0.993	0.993
AdaBoost	0.828	0.806	0.764

Для оцінки можливості підвищення швидкості роботи класифікатора проведено оптимізацію кількості ознак, які використовують для класифікації. Згідно з результатами табл. 2, в якості методу класифікації було обрано штучну нейронну мережу (ANN). В якості базового (максимального) використано набір даних, що містить 82 ознаки і дає точність 0.707 для тестового датасету (при розподілі навчального і тестового датасету 80%-20%).

Фільтрація класифікаційних ознак, які присутні лише в невеликій кількості пакетів, може потенційно прискорити процес класифікації та спростити налаштування системи за рахунок незначного погіршення точності. В даній

роботі запропоновано варіанти зменшення кількості ознак класифікації, які базуються на отриманих результатах аналізу груп характеристик. В результаті кількість ознак спочатку зменшено з 82 до 56 (табл. 3) з погіршенням точності з 0.707 до 0.683 (табл. 4). Цей набір ознак позначено як "середній". Наступним кроком виконано багатокритеріальну оптимізацію ознак класифікації шляхом перевірки рівня впливу кожної ознаки на точність та подальше зменшення кількості ознак з прийнятною втратою точності. В результаті отримано список з 18 найбільш важливих ознак (синій колір, курсів в табл. 3), який забезпечує точність 0.638 (табл. 4). Цей набір ознак позначено як "малий".

Таблиця 3. Набори ознак “середній” та “малий”

'Destination.IP', 'Destination.Port', 'Source.IP', 'Init_Win_bytes_forward', 'min_seg_size_forward', *'Fwd.Packet.Length.Max'*, 'Init_Win_bytes_backward', 'Flow.IAT.Max', *'Source.Port', 'Flow.Duration', 'Fwd.Packet.Length.Std', 'Bwd.IAT.Total',* 'Avg.Fwd.Segment.Size', 'Fwd.Packets.s', 'Fwd.IAT.Total', 'Fwd.IAT.Max', *'Fwd.Packet.Length.Mean', 'Subflow.Fwd.Bytes', 'Flow.Bytes.s',* 'Min.Packet.Length', 'Total.Length.of.Fwd.Packets', *'Bwd.IAT.Max',* 'Packet.Length.Variance', *'Bwd.Packets.s',* 'Flow.IAT.Mean', 'Fwd.Header.Length', 'act_data_pkt_fwd', 'Max.Packet.Length', *'Flow.Packets.s',* 'Flow.IAT.Std', 'Packet.Length.Std', 'Idle.Max', 'Fwd.Header.Length.1', 'Bwd.Packet.Length.Mean', *'Bwd.IAT.Std', 'Fwd.Packet.Length.Min',* 'Bwd.Packet.Length.Std', 'Avg.Bwd.Segment.Size', 'Average.Packet.Size', 'Total.Length.of.Bwd.Packets', 'Packet.Length.Mean', 'Fwd.IAT.Mean', 'Fwd.IAT.Std', 'Flow.IAT.Min', *'Bwd.IAT.Mean',* 'Bwd.Packet.Length.Max', *'Subflow.Fwd.Packets',* 'Total.Fwd.Packets', 'Total.Backward.Packets', 'Bwd.Header.Length', 'Subflow.Bwd.Bytes', 'Subflow.Bwd.Packets', 'Idle.Mean', 'Fwd.IAT.Min', 'Down.Up.Ratio', 'Idle.Min'

Для вказаних наборів ознак оцінено швидкість та точність класифікації в залежності від розміру датасету та значень гіперпараметрів, зокрема розміру вибірки та кількості епох (табл. 4). Збільшення розміру вибірки *batch size* (табл. 4) з 64 до 128 підвищує швидкодію з 105.1 сек до 67.7 сек, але точність погіршується з 0.699 до 0.683 (середній набір ознак). Збільшення кількості епох *epoch number* (10→100) покращує точність з 0.707 до 0.792, але час класифікації суттєво збільшується з 70.1 сек до 612.1 сек (базовий набір характеристик).

Під час оптимізації набору ознак необхідну кількість ознак зменшено з 82 до 18 (на 78%). Зменшення кількості ознак дозволило підвищити швидкість класифікації на 8% для великої кількості епох (50) і на 12% для кількості епох = 10, для гіперпараметра розмір вибірки 64.

Найвищу швидкість отримано при гіперпараметрах *batch/epoch* = 128/10, зменшивши кількість ознак до 54 (67.7 сек) та 18 (66.1 сек), однак це призводить до значного падіння точності до 0.683 та 0.611 відповідно.

Таким чином, якщо потрібна найвища продуктивність, рекомендовані налаштування: *batch/epoch* = 128/10 і використання малого (18) або середнього (54) набору ознак.

Найкраща точність досягається при збільшенні кількості епох і зменшенні параметра *batch*, що негативно впливає на продуктивність. Так, значення точності на тестовому наборі даних 0.794 досягається за ~1117 сек (при

batch/epoch = 64/100), що може бути неприйнятним, коли необхідно забезпечити низькі затримки в мережі 5G.

Таблиця 4. Точність та швидкодія класифікації в залежності від гіперпараметрів для алгоритму ANN

Batch size / epoch number	**Швидкодія класифікації / Точність (accuracy)**		
	Базовий набір ознак (82)	**Середній набір ознак (56)**	**Малий набір ознак (18)**
128 / 10	70.1s / 0.707	**67.7s / 0.683**	**66.09s / 0.638**
64 / 10	108.28s / 0.711	105.1s / 0.699	98.21s / 0.646
32 / 10	189.1s / 0.723	184.7s / 0.714	174.3s / 0.655
128 / 50	**322.3s /0.773**	304.7s /0.765	281.7s /0.700
64 / 50	718.2s / 0.775	578.6s / 0.770	513.9s / 0.705
32 / 50	1166s / 0.784	897.3s / 0.772	805.6s / 0.71
128 / 100	**612.1s / 0.792**	**601.1s / 0.779**	547.6s / 0.719
64 / 100	1117.8s / 0.794	1043.7s/ 0.788	984.8s/ 0.725

Загалом результати (табл. 4) показують, що зменшення кількості ознак до 18 не є ефективним, оскільки виграш у швидкодії не перекриває втрати в точності, майже всі результати малого набору ознак перекриваються результатами середнього набору ознак при інших значеннях гіперпараметрів.

4) Розробка нового методу обробки даних у вузлі мережі, який підвищує якість застосування технології граничних обчислень з множинним доступом (MEC, Mobile Edge Computing).

На цей час немає існуючих рішень, які б одночасно виконували перевірку справжності серверів розподілу та обчислювальних вузлів, керували процесом розподілу обчислювальних блоків, мали процедуру перевірки коректності розрахунків та враховували параметри обчислювальних вузлів під час розподілу.

Визначимо основних учасників процесу розподілених граничних обчислень (табл. 5) та їх функції згідно запропонованого в дисертації рішення.

Таблиця 5. Основні учасники процесу розподілених граничних обчислень

Учасник	Функції
MEC Сервер MEC	збирає потік даних з одного або більше датчиків/сенсорів; має радіомодуль з підтримкою 5G; може запустити додаток з підтримкою MEC; має мережний ідентифікатор та підтримує функції білінгу;
 Обчислювальний вузол	обробка виклику API користувача MEC; має радіомодуль з підтримкою 5G; має процесор, який підтримує роботу фреймворку MEC; має мережний ідентифікатор та підтримує функції білінгу;
 Базова станція	виділення радіоресурсу, перевірка особи, підписання транзакції, безпечне з'єднання; підтримка вибору обчислювального вузла; підтримка зв'язку точка-точка; забезпечення верифікованого зв’язку MEC Сервер -> Обчислювальний вузол;

В результаті врахування недоліків існуючих рішень запропоновано *метод обробки даних у вузлі інфокомунікаційної мережі*, який відрізняється наявністю процедур ідентифікації та автентифікації учасників розподілених периферійних обчислень, виділення додаткових ресурсів з мобільної мережі, включаючи процедуру підготовки зв'язку точка-точка, а також призначення обчислювальних вузлів і балансування навантаження між ними.

При цьому, для підготовки власного рішення, визначимо множину вхідних даних, набір обмежень, залежності між ними, а також множину вихідних значень.

Нехай на вхід системи розподілу навантаження для розподілених граничних обчислень поступають наступні дані:

n – множина доступних для МЕС обчислювальних вузлів з обчислювальними потужностями r_i та початкових рівнем довіри d_i;

di – початковий рівень довіри до обчислювального вузла;

$p(x_i)$ – ймовірність помилки під час розрахунків i-тим вузлом;

T_p – час на розподіл обчислювальних завдань;

Res – мережні ресурси задіяні під час розподілу завдань МЕС;

V – обсяг обчислень, які мають бути виконані.

Під час розподілу виконання обчислень, необхідно забезпечити мінімальну імовірність помилки розрахунків $p(i)$ (6) та мінімізувати використані ресурси мережі під часу розподілу і виконання обчислювальних завдань: $(Res \rightarrow min)$, за умови обмежень на очікуваний час обчислень ($T_o \leq T_{зад}$). Для визначення імовірності помилки розрахунків використовувалося середньозважене значення:

$$p_i = \frac{1}{n}\sum_i^n p(x_i), \tag{6}$$

В якості вихідних даних запропонований метод має надати:

$y \in n\{0,n\}$ – множину пристроїв, які виконують розрахунок розподілених обчислень з розподілом навантаження на основі потужностей r_i

$w \in n\{0,n\text{-}y\}$ – множину додаткових пристроїв, що забезпечують надмірність і надійність розподілених обчислень.

Δd_i – змінення рівня довіри до i-го вузла за результатами виконаної ним роботи;

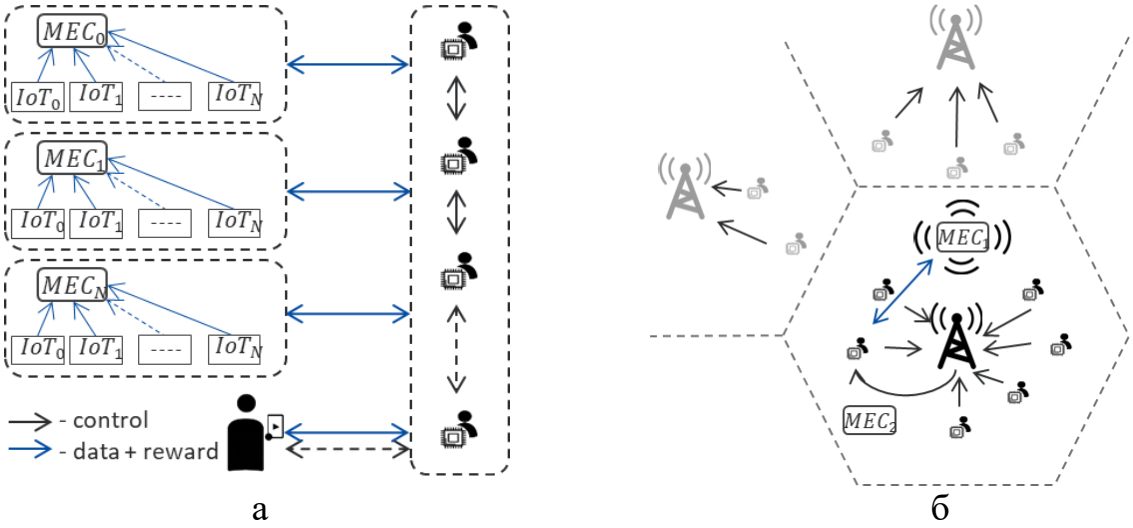
Очікуваний час обчислень буде складатися безпосередньо з часу виконання розрахунків і часу на розподіл обчислювальних завдань і може бути визначений як:

$$T_o = \frac{V}{n \cdot r} + T_\text{р}, \tag{7}$$

Або враховуючи множину пристроїв, які виконують розрахунок та множину додаткових пристроїв:

$$T_o = \frac{V}{\sum_i^y (y_i \cdot r_i) + \sum_i^w (w_i \cdot r_i)} + T_{\text{p}}. \quad (8)$$

Сутність описаного метода може бути проілюстрована за допомогою рис. 6а.



а б

Рис. 6. а) Візуалізація принципу роботи запропонованого методу; б) Послідовність дій на першому етапі (автентифікації і створення каналу)

Розглянемо сутність запропонованого методу:

1. Сервер MEC транслює запит на обчислення з наступною інформацією:
   - ідентифікатор MEC (тимчасовий або постійний ідентифікатор);
   - тип обчислення;
2. Кожен обчислювальний вузол, отримавши пейджинг, відповідає на нього базовій станції:

$$E = F(C_{id}, T_{last}, E_{id}), \quad (9)$$

де (C_{id}) – ідентифікатор стільника, що обслуговує (базової станції);
(T_{last}) – мітка часу останнього отриманого слоту для обчислень;
(E_{id}) – мережний ідентифікатор (тимчасовий або постійний).

3. Базова станція обирає обчислювальний вузол на основі отриманих значень E і призначає радіоканал, виходячи з наявних ресурсів. Після чого повідомляє про створений канал обміну сервер MEC та обчислювальний вузол.
4. Сервер MEC та обчислювальний вузол встановлюють з'єднання через радіоканал. Радіоканал формується на основі параметрів конфігурації каналу, які кожен з учасників отримує від базової станції.

5. Після цього сервер MEC та обчислювальний вузол виконують процедуру синхронізації.

6. На основі ETSI, обчислювальний вузол виконує API-дзвінок (рис. 7) і після завершення обчислень надсилає звіт до базової станції;

7. Після перевірки результату, сервер MEC звітує базовій станції.

Рис. 7. Запропонована послідовність дій під час API-дзвінка

Оскільки результати обчислень несуть ризики обчислювальних помилок внаслідок збоїв та різного роду атак, то запропонований метод передбачає перевірку результатів роботи, аналіз рівнів довіри та внесення надмірності в процедуру обчислень, що реалізується наступними етапами:

1) обчислювальний пристрій сервера MEC генерує код контролю помилок, як набір функцій низького обчислювального рівня. Код контролю помилок – це автоматично створене завдання з такою ж складністю, форматом і довжиною вхідних даних, як і реальне завдання, з тією відмінністю, що сервер MEC знає точний результат, тому його можна перевірити.

2) обчислювальний пристрій сервера MEC розподіляє завдання між обчислювальними вузлами MEC з додатковою надмірністю. Додаткова надмірність допомагає уникнути випадкових помилок в обчисленнях, які можуть виникнути навіть на перевірених вузлах. Сервер MEC застосує результати роботи і надає винагороду тільки після того, як принаймні 51% вузлів, що отримали однакове завдання надішлють такі ж результати.

3) сервер MEC оновлює свій рівень довіри після успішного виконання завдання. Кожен сервер MEC має власний "рівень довіри" d_i, який залежить від виконання контрольного коду та результатів раніше виконаних завдань. Якщо результати виконання контрольного коду правильні, рівень довіри для цього обчислювального вузла підвищується. В іншому випадку, якщо пристрій

обчислює контрольний код з помилками, рівень довіри знижується до повного блокування вузла.

Запропонований метод обробки даних дозволяє організувати розподілені граничні обчислення в 5G мережі і надає переваги як користувачам так і мобільному оператору. Користувачу метод забезпечує:

• Простоту налаштування: як ідентифікатор обладнання користувача можна використовувати звичайні мережні ідентифікатори або номер блокчейн-гаманця.

• Високий рівень безпеки та надійності: транзакція підписується за допомогою технології блокчейн. Виконується перевірка даних і контрольний код для захисту від шахрайства та виявлення помилок.

Мобільному оператору це дозволяє економити мережні ресурси (порівняно з існуючими рішеннями, оскільки динамічна карта зі списком вузлів або інша база даних / маршрутна таблиця не потрібна); знизити вартість (не потрібно додаткового апаратного забезпечення), легко обирати обчислювальні вузли і балансувати навантаження MEC (базова станція приймає рішення на основі правил та набору обчислювальних вимог), а також зменшити навантаження на мобільну мережу, оскільки зв'язок точка-точка, передбачений в 5G, відбувається без участі базової станції.

В **розділі 4** описано *вдосконалення моделей та методів завадостійкого кодування пакетів під час їх передачі мобільною мережею для зменшення рівня помилок і втрат пакетів*. Вдосконалення завадостійкого кодування полягає у новій моделі формування коду Raptor і обгрунтуванні вибору його елементів.

Raptor код є розширенням коду LT, в рамках 3GPP, коди Raptor використовуються для надійної доставки даних в мобільних та бездротових мережах, широковіщальній і груповій доставці. Raptor коди відносяться до каскадних кодів. Символи даних по-перше попередньо кодуються зовнішнім кодом. Вихідні символи прекодеру називаються проміжними символами, і вони являються вхідними символами внутрішнього коду LT. Прекодер – код з фіксованими параметрами, як правило, з досить високою швидкістю. Прекодер може бути багатоступеневим, тобто попередньо код може бути сумою кількох кодів з фіксованими параметрами.

5.1) Вдосконалення моделі формування коду Raptor.

В даній роботі запропоновано вдосконалення моделі Raptor кодів шляхом внесення процедури перемежіння і змін у матриці формування коду. Синтезована модель наведена на рис. 8. В якості вхідних даних використовується довжина повідомлення k, довжина кодового слова n і фактор витрат на кодування ε. Кожну частину конструкції коду відтворено в симуляторі, щоб проаналізувати різні аспекти його продуктивності.

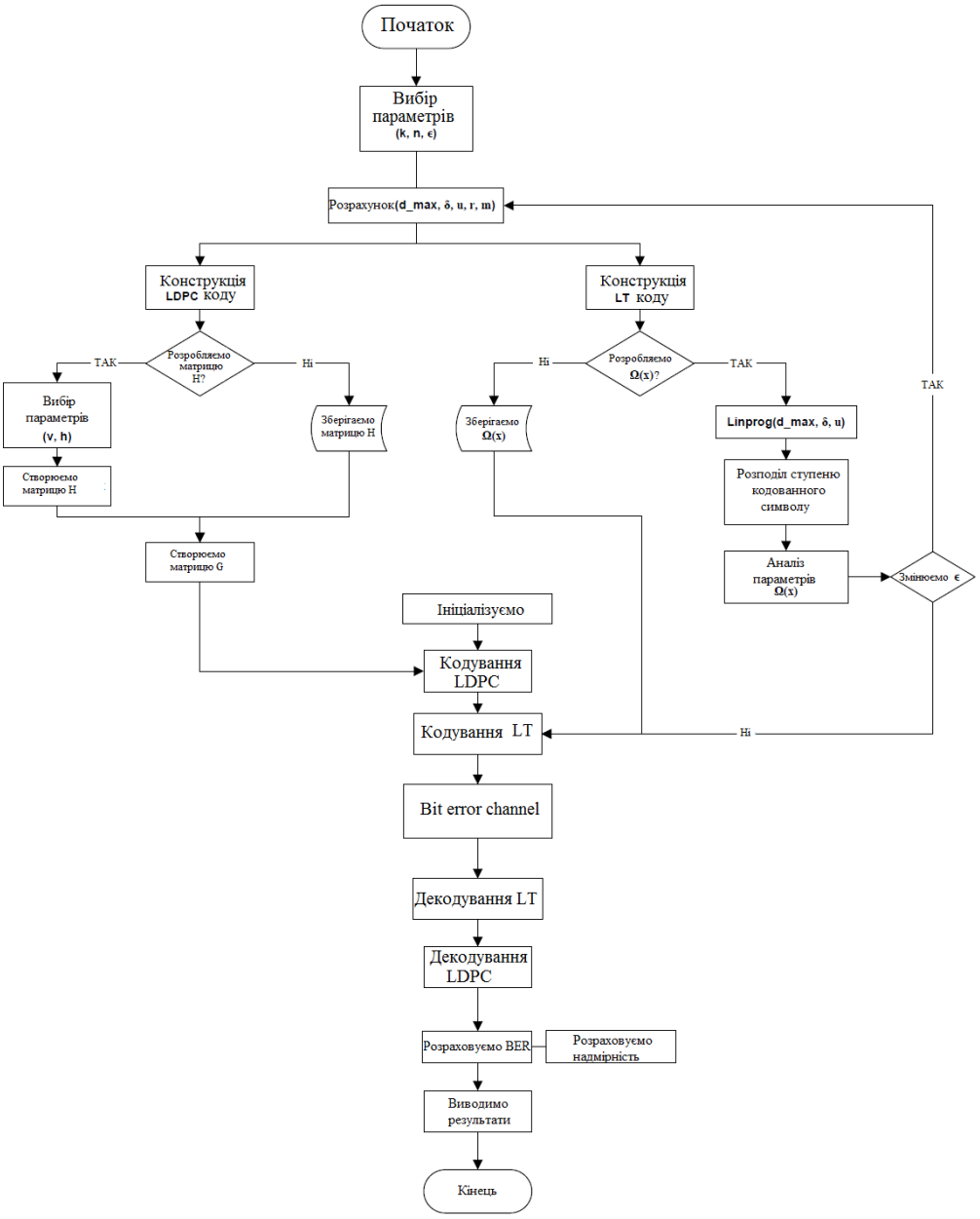


Рис. 8. Алгоритм запропонованої модифікації Raptor коду

5.2) Вибір характеристик і моделювання елементів коду Raptor на тлі каналів з завадами

З отриманих результатів, можна зробити висновок, що кращі властивості декодування забезпечує LDPC-код. Він дозволяє виправляти передане повідомлення з дисперсією помилки 0.415 від амплітуди сигналу в каналі з АБГШ, з імовірністю помилки 0.390 в каналі з мультиплікативної помилкою і ймовірністю помилки 0.357 в каналі зі стираннями (з урахуванням використання перемежіння).

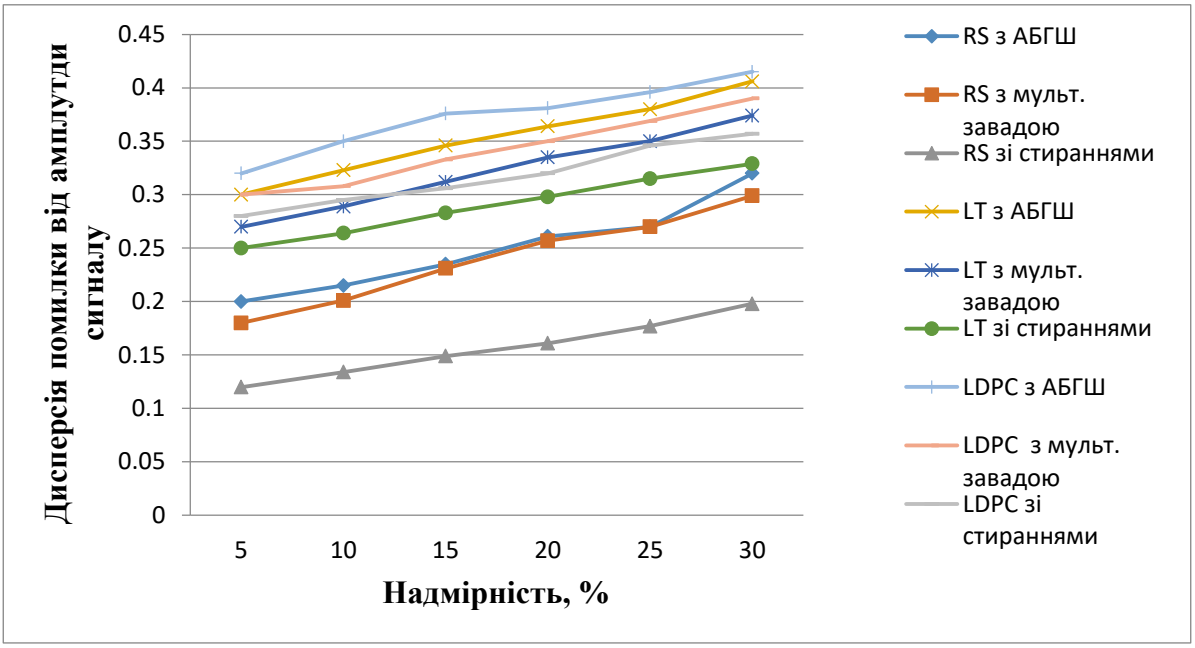


Рис. 9. Результати моделювання

Моделювання проводилося з показником надмірності рівним 10%. Час витрачається на кодування і декодування повідомлень у LT-коду значно менше, ніж у кодів Ріда-Соломона і LDPC (табл. 6, 7).

Таблиця 6. Час затрачений на перемежіння та деперемежіння залежно від розміру файлу

Розмір файлу, Мб	Час затрачений на перемежіння файлу, с.	Час затрачений на деперемежіння файлу, с.
0.25	0.02	0.015
0.5	0.0185	0.0176
1	0.0374	0.0362
2	0.069	0.061
4	0.12	0.112
8	0.202	0.196
16	0.389	0.37

Для кодування і декодування, а також перемежіння і деперемежіння повідомлень розміром 16 Мб LT-коди потребують 1.51с. і 1.34с. відповідно, у той час коли для кодування і декодування кодом Ріда-Соломона необхідно затратити 6156.39 с. і 4212.37 с. відповідно.

LDPC коди витрачають на дані дії 31.1с і 28.3с. Виходячи з отриманих результатів, кращі характеристики по швидкодії забезпечують LT-коди, які дозволяють виправляти більшу кількість помилок в мережі передачі даних, а також використовувати менше часу на кодування і декодування, з урахуванням перемежіння і деперемежіння (у порівнянні з кодами Ріда-Соломона і LDPC).

Таблиця 7. Залежність затрат часу від розміру файлу

Розмір файлу, МБ	Затрачений час, с.					
	Код Ріда-Соломона		LDPC код		LT код	
	Кодув. + перемеж.	Декод. + деперемеж.	Кодув. + перемеж.	Декод. + деперемеж.	Кодув. + перемеж.	Декодув. + деперемеж.
0.25	4.62	2.07	1.75	1.01	0.05	0.035
0.5	19.02	8.42	2.92	2.12	0.06	0.055
1	77.04	40.53	5.16	3.93	0.11	0.103
2	301.07	124.06	9.16	6.86	0.26	0.16
4	912.12	456.11	15.49	10.02	0.53	0.30
8	2546.2	1487.2	20.51	15.79	1.07	0.65
16	6156.39	4212.37	31.15	28.33	1.51	134

На основі цього можна зробити висновок, що в даних реалізаціях LDPC коди є більш надійними ніж коди Ріда-Соломона і LT, дозволяє виправляти більшу кількість помилок при однаковій надмірності, але LDPC коди програють по швидкодії реалізації кодування-декодування і перемежіння кодом LT. Тому враховуючи специфіку мереж 5G і необхідність мінімізації затримки, рекомендується використовувати Raptor коди на основі комбінації LT та LDPC.

Також з результатів моделювання можна зробити висновок, що використання методів перемежіння на 11% дозволяють поліпшити виправлення помилки в переданому повідомленні у порівнянні з існуючими результатами.

В **розділі 5** описано нові моделі та методи захисту приватних даних у пристрої користувача, які відрізняються наявністю нових методів формування біометричного шаблону, об'єднання різних типів біометричних даних, запропонованого завадостійкого методу приховання біометричних даних під час передачі, а також забезпечення двобічної автентифікації та наскрізного шифрування під час дзвінка, що дозволяє уникнути підміни користувача на іншому боці і отримати доступ до сервісів лише авторизованому користувачу, що підвищує на один рівень надання послуг показників конфіденційності, цілісності та спостереженості.

6) Вдосконалення методу формування біометричного шаблону користувача і агрегацію різних біометричних ознак користувача.

Наявні методи формування біометричних шаблонів, як правило, використовують одну біометричну ознаку, агрегація ознак, яка б надала змогу підвищити рівень захищеності відсутня, або відбувається без визначення пріоритетів та оцінювання поточного стану зовнішнього середовища, в якому знаходиться користувач. Агрегація біометричних ознак дозволяє використовувати саме ті біометричні ознаки в даний момент часу, які є найбільш зручними для користувача і при цьому вони мають забезпечити заданий рівень захищеності.

Метод застосовує відомі блоки попередньої обробки, отримання ознак, формування вектору ознак. Після цього дані з різних біометричних сенсорів

потрапляють на *запропонований модуль агрегації* і за результатами його роботи формується криптографічний ключ.

Попередня обробка даних включає вибір необхідного типу біометрії і отримання інформації від потрібних сенсорів. Під час отримання ознак, дані з сенсорів трансформуються в набір ознак, відповідно до алгоритму обробки даного типу біометрії. Після отримання набору ознак, він перетворюється на вектор ознак, що буде мати фіксований розмір (рис. 10).

Запропонований модуль агрегації отримує на вхід вектори ознак з виходу модулів формування вектору ознак (рис. 11).

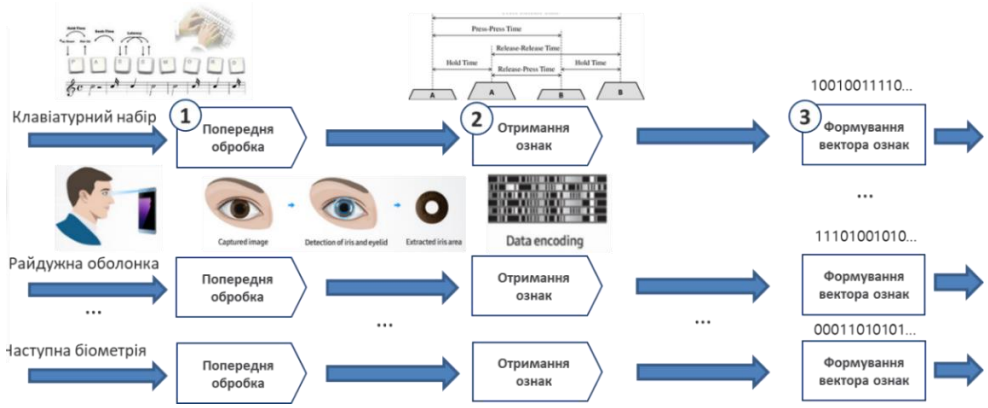


Рис. 10. Основні перетворення модуля формування вектору ознак

До задач модуля агрегації входить поєднання різних типів біометричних даних в єдину структуру, забезпечення конфіденційності та цілісності даних користувача при обміні, а також забезпечення стійкості до завад під час передачі відкритими каналами.

Рис. 11. Запропонована структура модуля агрегації біометричних ознак

Принцип роботи модуля агрегації полягає в наступному (рис. 11):

1) Отримання сформованих векторів ознак від модулів їх формування. Визначення наявних типів біометричних даних.

2) Для формування криптографічного ключа або проходження автентифікації необхідно перевищити порогове значення. Кожен тип біометрії має власний пріоритет (рівень довіри) і відповідну вагу. Застосування *вектору*

пріоритетів дозволяє визначити важливість певного методу біометричної автентифікації і його вплив на підсумковий результат.

3) Вибір тих біометричних даних, які мають забезпечити перевищення порогового значення, необхідного для певного додатку користувача відповідно до заздалегідь заданого набору правил.

4) Застосування *генератора шуму* для зашумлення тих полів, що не використовуються під час даної сесії (але за умови використання іншої біометрії наступного разу – можуть бути заповненими). Це не дозволяє злонамірнику винайти зв'язок між полями.

5) Оскільки криптографічний ключ має передаватися по відкритим каналам мобільного зв'язку для виконання віддаленої автентифікації, то необхідно забезпечити його стійкість до завад в каналі. Цю задачу вирішує *блок перемежіння*. Додатковою його задачею є підвищення прихованості.

6) Використання *завадостійкого коду* після перемежіння має на меті підвищити стійкість до завад. На цьому етапі пропонується використовувати модифікований варіант коду Raptor, який описано вище.

7) Параметри завадостійкого коду залежать від параметрів каналу зв'язку, які через петлю зворотного зв'язку потрапляють на кодер (*блок оцінка якості параметрів каналу*) і запропонована інтелектуальна система прийняття рішень налаштовує параметри завадостійкого кодування та обирає тип біометричної системи для формування шаблону.

Розглянемо запропоновану систему прийняття рішень. Нехай на її вхід подається набір вхідних даних, який для досліджуваного випадку містить інформацію про стан каналу зв'язку та інформацію про характер отриманих біометричних ознак користувача. Інформація про стан каналу включає наступні параметри (дослідження проводилися на прикладі LTE/5G мережі):

- параметри потужності сигналу та якості: потужність сигналу NR-RSRP/RSRP (Reference Signal Receive Power), якість сигналу RSRQ (Reference Signal Received Quality), співвідношення сигнал/шум SINR (Signal-to-Interference-plus-Noise Ratio), доступна пропускна здатність Cell Bandwidth, використовувана схема модуляції та кодування MCS (Modulation and Coding Scheme);

- наявність фонових сесій за протоколами IP, TCP, RTP, SCTP та ін.

На основі пропускної здатності, співвідношення сигнал/шум та параметрів якості/потужності визначаються рекомендовані параметри завадостійкого кодування, а також гранична кількість повторно переданих пакетів. Цей набір є вхідною інформацією для штучної нейронної мережі, яка використовує його для вибору найкращого методу захисту даних та методу приховування (вбудовування) даних. Так, в запропонованій системі додатково аналізується наявність активних сесій, що впливає на вибір методу приховування.

Для навчання штучної мережі була підготовлена вибірка мережних станів, отримана з телефонів Samsung Galaxy S21, яка містить стани каналу від RSRP =

–60 дБм до –120 дБм, якість RSRQ змінюється в діапазоні від –5 до –18 дБ, виділена смуга частот: 10-15МГц. Перед початком роботи інтелектуальної системи формуються всі дозволені сценарії роботи. Множина сценаріїв зберігається у спеціальній базі знань. Архітектура бази даних включає всі зазначені поля стану каналу, також до неї включені поле з переліком можливих методів захисту та поле з набором дозволених алгоритмів. Обрання того або іншого сценарію відбувається на основі навчання нейронної мережі. Для недопущення випадку DoS (denial of service) атаки в базі знань має бути прописаний «найгірший» сценарій, який працюватиме у будь-яких умовах, але можливо з гіршими характеристиками (нижча швидкість та прихованість, більша надмірність шаблону). Використовуючи вхідні дані система обирає сценарій, який максимально відповідає поточному стану згідно заданих заздалегідь критеріїв відповідності. Після цього з бази знань обирається набір доступних для цього сценарію методів захисту.

Приклад роботи системи і формування рішення наведено на рис. 12. У наведеному прикладі маємо низький рівень потужності при низькій якості, що буде відповідати параметру якості каналу (CQI) 7-9. Це призведе до обрання алгоритму модуляції 16QAM і швидкості кодування 1/3, також немає інформації про додаткові сесії, відповідно обрано стійкий до завад алгоритм захисту – біометрична система зі зв’язуванням ключа.

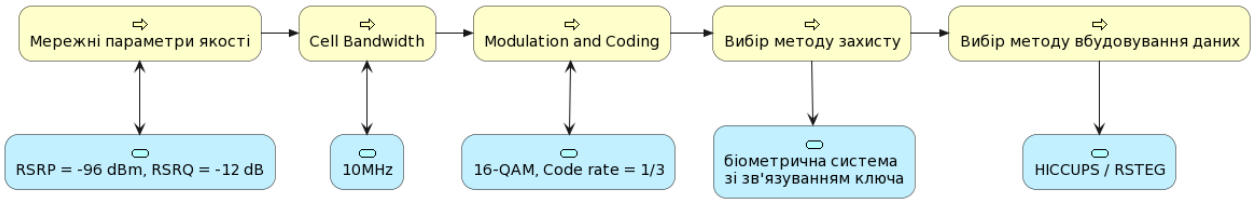


Рис. 12. Приклад роботи інтелектуальної системи прийняття рішень

Запропонований метод дозволяє використовувати біометричні ознаки для віддаленої автентифікації та формування криптографічного ключа без ризику їх компрометації. Також на основі інформації о наявних біометричних ознаках користувача обирається найкращий за заданими критеріями спосіб їх перетворення в захищений біометричний шаблон.

7) Вдосконалення процедури віддаленої автентифікації шляхом застосування методів мережної стеганографії та завадостійкого кодування, що дозволило підвищити прихованість та завадозахищеність інформації.

Для підвищення захищеності (шляхом збільшення прихованості) біометричних даних можливе використання різних методів стеганографії, які дозволяють скрити сам факт передачі даних, необхідних для автентифікації через мережу. Інформація, факт передачі якої потрібно приховати, розміщується в стегоконтейнері, в якості якого можуть виступати аудіо та відео файли, зображення, мережеві заголовки та інша інформація, яка має

надмірність. Модифікація таких контейнерів незначна і факт приховування в них даних складно виявити.

В роботі методом багатокритеріальної оптимізації оцінено ефективність застосування методів мережної стеганографії в системі віддаленої автентифікації. Для цього використані характеристики методів стеганографії і сформовані матриці попарних порівнянь (10):

$$A = \begin{pmatrix} 1 a_{12} \ldots a_{1j} \\ a_{21} 1 \ldots a_{2j} \\ \ldots \\ a_{i1} a_{i2} \ldots 1 \end{pmatrix}, \tag{10}$$

де $a_{ij} = \frac{w_з}{w_j}$ – значення, що відображає ступінь переваги одного показника над іншим. На основі (10), оцінено власні вектори V_i показників (11) і глобальний вектор пріоритетів P_j (12):

$$V_j = \sqrt[n]{\prod_{i=1}^{n} a_{ij}}, \quad j = \overline{1,n}, \tag{11}$$

де n – кількість показників.

$$P_j = \frac{V_j}{S}, \quad j = \overline{1,n}, \text{ де } S = \sum_{j=1}^{n} V_j. \tag{12}$$

Результати розрахунку і аналізу ефективності застосування методів мережної стеганографії наведені в табл. 8.

На основі визначеного переважного методу мережної стеганографії запропоновано схему захисту процесу віддаленої біометричної автентифікації з додаванням етапів приховування та завадостійкого кодування. Блоки, які відрізняють її від існуючої системи наведені зеленим кольором (рис. 13).

Таблиця 8. Вектори пріоритетів методів мережної стеганографії

№	Метод	Глобальний вектор пріоритету
1	**TranSteg**	**0,162**
2	LACK	0,116
3	**HICCUPS**	**0,165**
4	RSTEG	0,059
5	**Модифікація заголовків TCP/IP/RTP**	**0,171**
6	Модифікація блоків даних SCTP	0,082
7	SCTP (гібрид)	0,114
8	SCTP multi-homing	0,129

Оскільки є декілька методів мережної стеганографії зі схожим значенням глобального вектору пріоритетів, вибір може бути оптимізований в певний момент часу, в залежності від стану каналу зв’язку і наявності активних сесій. Це знайшло відображення у вдосконаленні наведеної вище інтелектуальної системи (рис. 12). Вдосконалення полягало у виборі набору методів захисту, на основі ідентифікації умов на вході і визначенні поточного сценарію. При цьому, аналіз наявності фонових сесій за протоколами IP, TCP, RTP, SCTP, дозволяє обрати під наявну сесію переважний метод мережної стеганографії.

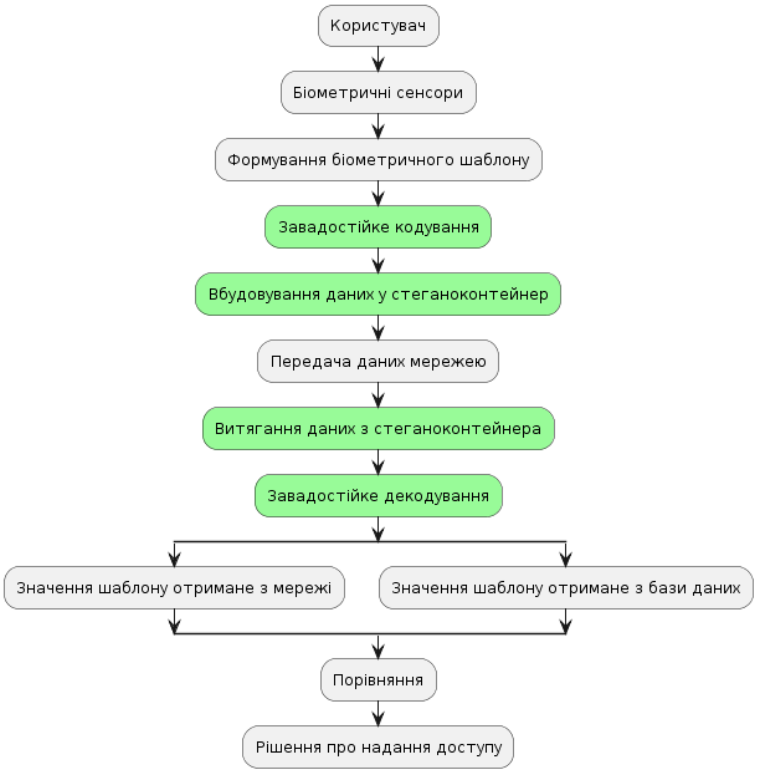


Рис. 13. Модифікована схема віддаленої біометричної автентифікації

Вказаний підхід впроваджено в систему приховання біометричних даних користувача у зображеннях за допомогою цифрових водяних знаків. Згідно запатентованого у співавторстві рішення (рис. 14), пропонується на зображеннях користувача знаходити біометричні ознаки методами комп’ютерного зору, кодувати винайдені біометричні ознаки і генерувати нове зображення з модифікованими біометричними ознаками та цифровим водяним знаком. Після цього у соціальних мережах або відкритих публікаціях початкове фото замінюється на синтезоване. Для шифрування водяного знаку використовується секретний ключ пристрою. Цей ключ зберігається в довірчій зоні і вважається захищеним. Процедура шифрування та дешифрування також виконується в довірчій зоні ("безпечному світі").

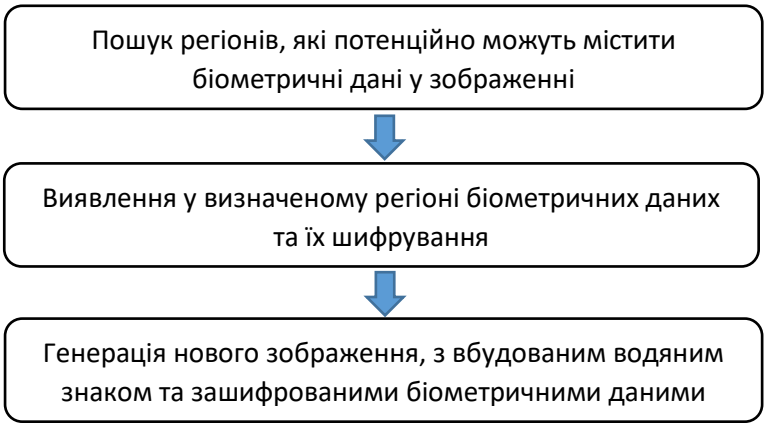


Рис. 14. Алгоритм модифікації біометричних ознак у зображенні

8) Розробка нового методу взаємної автентифікації користувачів під час дзвінка, що перекриває ряд загроз пов'язаних із шахрайськими схемами підміни користувача.

В існуючих мережах є багато рішень направлених на вирішення завдань автентифікації користувача, але всі вони мають ряд недоліків і не забезпечують захисту при наступних сценаріях:

- з довіреного номера дзвонить інша людина (в існуючих рішеннях виконується автентифікація пристрою а не користувача);
- на приймальному боці трубку знімає не власник телефону, що може привести до витоку конфіденційної інформації;
- відбувається спуфинг (підміна) номера;
- відбувається витік даних на боці довірчої третьої сторони.

Для перекриття цих недоліків запропоновано метод забезпечення взаємної автентифікації без зберігання конфіденційної інформації на боці «довірчої третьої сторони». В якості вимог до методу запобігання спам-дзвінків, ободзвінків та вішингу були обрані:

- взаємна автентифікація користувачів під час дзвінка;
- сумісність з дзвінками 3G/2G (CS-дзвінки) і VoIP/SIP (PS-дзвінки);
- автентифікація має виконуватися природно, без додаткових дій з боку користувача;
- неможливість прийняти дзвінок без проходження автентифікації користувача.

Сутність методу безпечної відповіді на дзвінки полягає в (рис. 15):

1. отриманні біометричних даних користувача, що підлягає автентифікації (фаза реєстрації);
2. автентифікації користувача ПІД ЧАС ДЗВІНКУ (без додаткових дій), на основі біометричних даних;
3. у разі позитивної автентифікації:

a. повідомлення з результатом автентифікації буде надіслано обом сторонам;
b. на екрані обох абонентів з'являється підтвердження автентифікації;
c. виклик може бути прийнятий або відхилений відповідно до рішення авторизованого користувача;

4. у разі негативної автентифікації:
a. вхідний дзвінок буде відхилено;
b. або може бути запитано додаткову автентифікацію.

Описану вище послідовність реалізує метод, зображений на рис. 16. Зеленим кольором позначені вдосконалені або вперше запропоновані елементи.

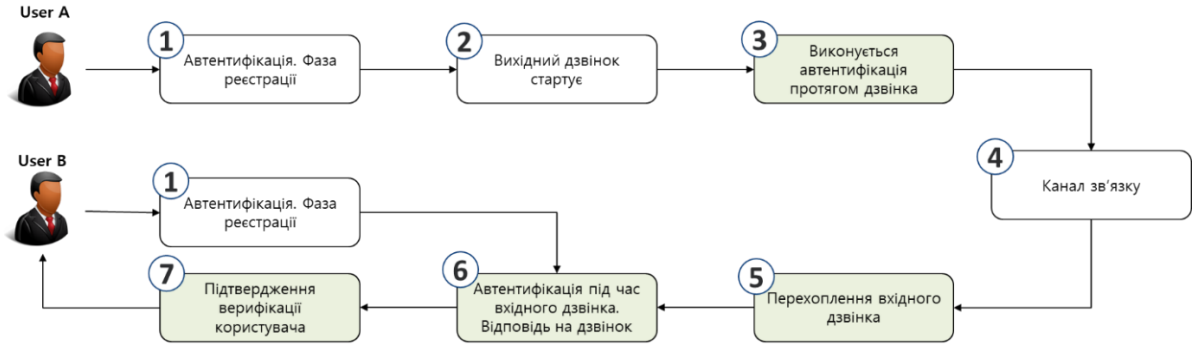


Рис. 15. Запропонований метод безпечної відповіді на дзвінки шляхом взаємної автентифікації користувачів

Відповідно до рис. 15 сценарій використання запропонованого методу складається з наступних етапів:

1. *Автентифікація: фаза реєстрації* полягає в тому, що користувачу потрібно вперше пройти процедуру реєстрації для автентифікації за малюнком вуха. Щоб це зробити, користувач робить запит на процедуру автентифікації в додатку.

2. *Початок вихідного дзвінка*. Після успішної фази реєстрації користувач починає дзвінок через стандартний додаток.

3. *Автентифікація протягом вихідного дзвінка*. Новий запропонований елемент алгоритму полягає у застосуванні автентифікації по малюнку вуха під час набору номера. Автентифікація по малюнку вуха була обрана базуючись на описаних в роботі перевагах. У випадку її неуспішності може застосовуватись автентифікація через акустичний відгук або відбиток пальця.

4. *Канал зв'язку*. Виконується типові мережні процедури, пов'язані з передачею інформації від користувача *A* до користувача *B* і у зворотному боці.

5. *Перехоплення вхідного дзвінка*. Новий запропонований елемент алгоритму. Відповідає за автентифікацію користувача, який приймає дзвінок. Повідомлення про успішне проходження автентифікації включається до повідомлення “Connect” і відправляється на сторону абонента, що дзвонить. У випадку неуспішної автентифікації користувачу пропонується інший спосіб

верифікації (наприклад відбиток пальця). До успішної автентифікації дзвінок не може бути прийнятий і буде відхилений.

6. *Відповідь на вхідний дзвінок* дозволяється тільки після успішної автентифікації.

7. *Підтвердження про верифікацію користувача* відбувається після успішної автентифікації під час дзвінка. Підтвердження для обох користувачів будуть доставлені за допомогою повідомлень SETUP і CONNECT ACK.

Підсумкова діаграма повідомлень (call flow), що відображає весь процес дзвінка з вказанням модифікованих елементів (зелений колір) наведена на рис.16. Для захищеної передачі повідомлень взаємної автентифікації використовується короткий автентифікаційний рядок (SAS). Запропонований метод дозволяє забезпечити високорівневу реалізацію послуг «автентифікація відправника» та «автентифікація отримувача».

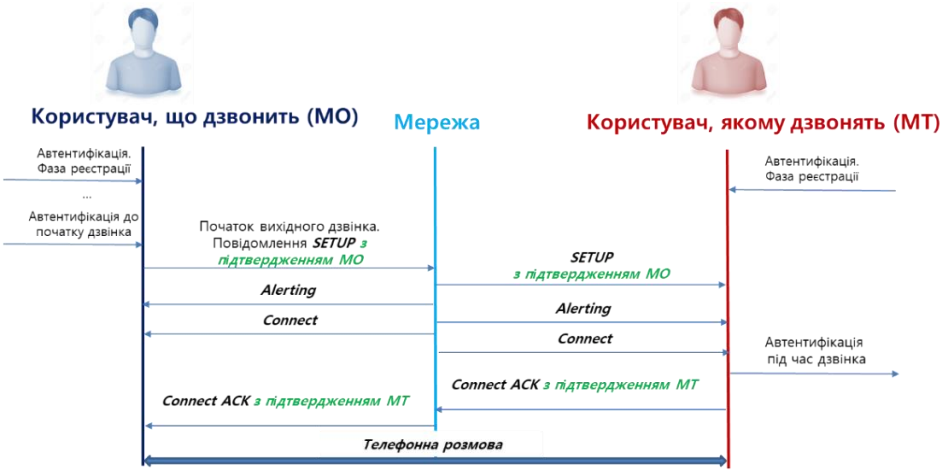


Рис. 16. Модифікований протокол обміну повідомленнями під час проходження голосового дзвінка через мережу

9) Вдосконалення існуючих протоколів обміну повідомленнями під час дзвінка шляхом застосування процедур наскрізного шифрування та перевірки цілісності для підвищення рівня захищеності під час передачі даних в 5G мережі.

Окрім задачі взаємної автентифікації користувачів, під час дзвінка користувачі стикаються ще з рядом проблем, до яких відносяться:

- наскрізне шифрування в мобільній мережі відсутнє;
- голосові дані користувача (включаючи паролі) можуть бути перехоплені;
- абоненти мобільної мережі не захищені від сніфінг-атаки з боку оператора;
- абоненти мобільної мережі не захищені від атаки створення хибної базової станції і інших атак.

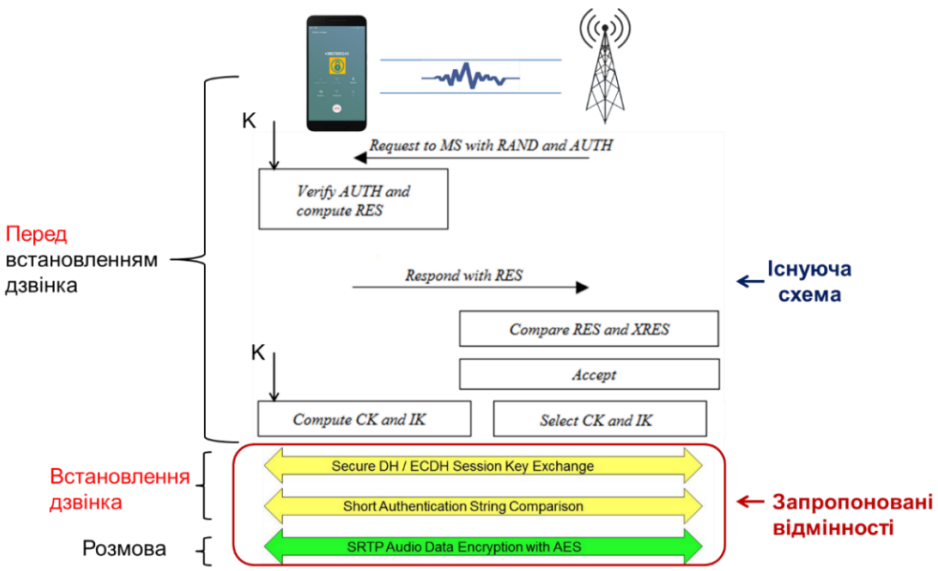


Рис. 17. Вдосконалена процедура забезпечення конфіденційності абонента

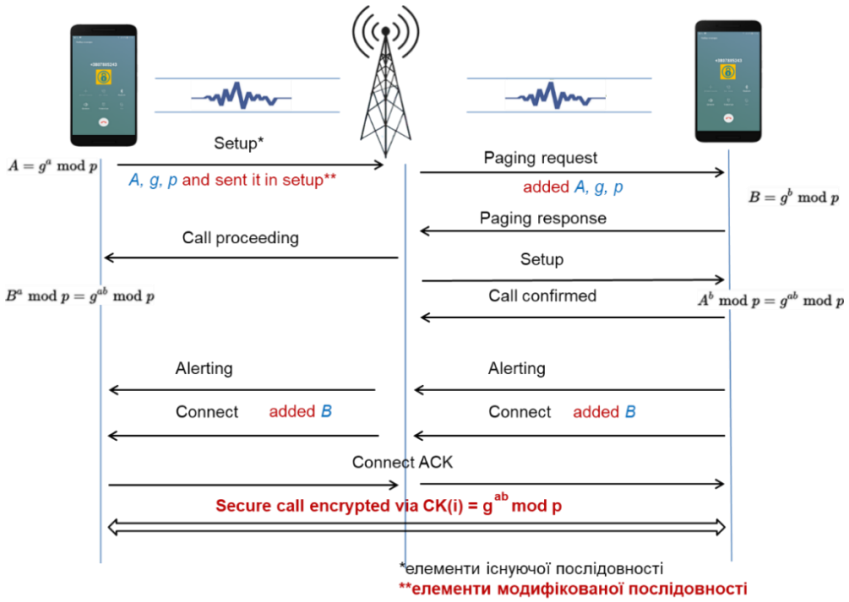


Рис. 18. Імплементація протоколу обміну ключами Діффі-Хелмана в протокол обміну повідомленнями

Перекриття наведених вище атак досягається шляхом реалізації наступних запропонованих під час дзвінка відмінностей (рис. 17):

- протоколу Діффі-Хелмана для безпечного обміну ключами;
- короткого автентифікаційного рядка (SAS) для протидії атаці "зловмисника посередині";
- використанні хешу попереднього дзвінка для протидії спуфінгу телефонних номерів;

- використанні сучасного симетричного шифрування мови алгоритмом AES(256) для протидії прослуховуванню і підвищенню конфіденційності при обміні.

Для реалізації протоколу обміну ключами Діффі-Хелмана запропоновано модифікація повідомлень SETUP і CONNECT в традиційній послідовності повідомлень (call flow) під час встановлення дзвінка. Модифікована послідовність наведена на рис. 18. Обмін ключами Діффі-Хеллмана не забезпечує захист від атаки "зловмисника посередині". Щоб переконатися, що зловмисник дійсно не присутній в першій сесії (коли немає спільних секретів), запропоновано використання короткого автентифікаційного рядка (SAS). Послідовність дій під час розрахунку і використання SAS, наведена на рис. 19. Запропоновані відмінності позначені червоним кольором.

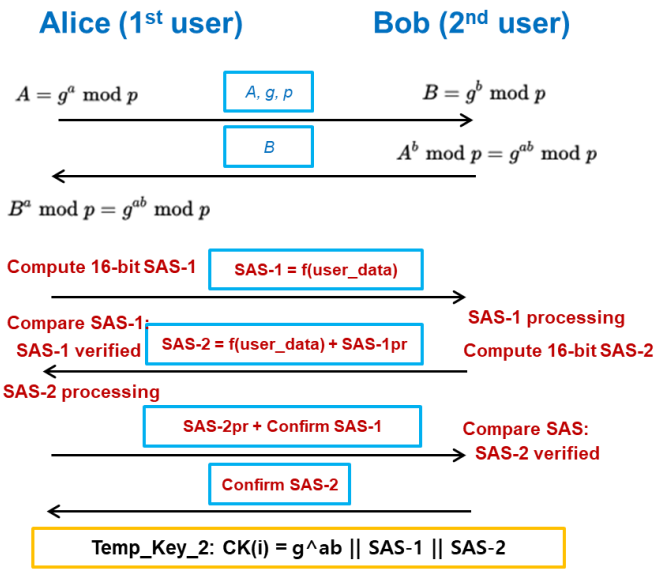


Рис. 19. Послідовність дій під час розрахунку і використання SAS

Ефективність протидії атакам "зловмисник посередині" (MitM) досягається впровадженням другого рівня автентифікації, заснованому на певній формі неперервності ключа. Для цього в TrustZone зберігається хешована ключова інформація для використання в наступному виклику, яка буде змішана з загальним секретом DH наступного виклику, що надає йому властивості неперервності ключа, аналогічні протоколу SSH.

Таким чином сутність запропонованого методу полягає у наступному:

- обчислення тимчасового ключа для першого користувача з ключового матеріалу першого користувача та випадкових криптографічних даних через TrustZone для безпечного мобільного дзвінка;

- надсилання ключового матеріалу другому користувачу;

- генерування сеансового ключа з тимчасових ключів першого користувача та другого користувача для шифрування мобільного голосового дзвінка між першим користувачем та другим користувачем;

- використання короткого автентифікаційного рядка (SAS) для захисту від атак типу "зловмисник посередині" (MitM);

- зберігання в пам'яті хеш-значення для попередніх захищених викликів;

- доповнення матеріалу криптографічного ключа під час другого сеансу зв'язку між першим користувачем і другим користувачем матеріалом криптографічного ключа з першого сеансу зв'язку.

Впровадження описаного методу реалізує на вищому рівні послуги «конфіденційність при обміні» і «цілісність при обміні», що забезпечує підвищення загального рівня конфіденційності.

10) Розробка моделей управління приватними даними користувача для забезпечення захищеності даних під час реалізації нових сервісів.

Для реалізації нової моделі управління і надання користувачу додаткових можливостей без зниження рівня захищеності, в даній роботі запропоновано два методи. Перший пропонує використання біометричної автентифікації, машинного навчання та розпізнавання зображень для надання користувачу можливості віддаленого управління об’єктами. Другий – метод зберігання приватних даних користувача в захищеному ієрархічному вигляді і дозволяє надавати доступ до них різного рівня у надзвичайних випадках для збереження життя користувача.

Перший метод являє собою спосіб і пристрій для збору, зберігання і представлення конфіденційної інформації користувача, пов'язаної з візуально розпізнаними об'єктами (наприклад, системами кондиціонування повітря і іншими пристроями розумного будинку, які можуть працювати в мережі 5G). Запропонований метод включає етапи ідентифікації та автентифікації користувача на пристрої, розпізнавання певного об'єкта, зберігання розпізнаних об'єктів та секретної інформації, порівняння збережених розпізнаних об'єктів з вхідними, пошук інформації, пов'язаної з розпізнаним об'єктом, та виконання дії, пов'язаної з об'єктом. Структурна схема системи показана на рис. 21. Зображення або відео знімається за допомогою камери. Крім того, зображення/відео можуть зберігатися на блоці репозиторію, наприклад, з додатку галереї на смартфоні або бути частиною програми, запущеної на електронному пристрої, наприклад, програми електронної пошти із зображенням як вкладенням. Блок оптичного розпізнавання виконує розпізнавання об'єктів.

Користувач виконує автентифікацію у блоці біометричної автентифікації. Виконується запит на пошук об'єктів у базі даних. Результати пошукового запиту представляються користувачеві. У деяких варіантах реалізації це просто дія відображення: відображення результату пошуку користувачеві. В інших варіантах реалізації дії можуть виконуватися для управління або обміну інформацією з додатками, що працюють на електронному пристрої. У третіх варіантах результат пошукового запиту виводиться за допомогою

передавального пристрою. Пристрій передачі може бути будь-яким з WIFI, NFC, RFID, BLE, Bluetooth, ZigBee тощо.

Рис. 20. Елементи запропонованого методу управління об’єктами

Другий запропонований метод пов’язаний з індивідуальною медичною базою даних, яка не є однорідною і складається з різної інформації з різним рівнем безпеки. Наприклад, особиста інформація користувача, така як ім'я, адреса, група крові, не є дуже секретною, але вона не повинна бути доступною для всіх. Інші типи інформації – хронічні захворювання та алергії – можуть бути доступними лише для спеціальних осіб, коли це дійсно необхідно. Третій тип медичної інформації, такий як історія хвороби, може бути наданий лише безпосередньо довіреному медичному центру. Відповідно до цих різних типів інформації можуть застосовуватися різні типи безпеки та різні ключі шифрування/розшифрування. Пристрої користувача можуть визначати, кому і яку інформацію надавати. Запропоноване рішення реалізує ієрархічну систему зберігання медичних даних. Особливості такого зберігання полягають у наступному: персональні дані класифікуються відповідно до одного з трьох рівнів даних і не дублюються; кожен з рівнів даних шифрується власним ключем, відповідно до рівня доступу, при цьому на кожному рівні даних зберігається ключ нижчого рівня.

ВИСНОВКИ ТА РЕЗУЛЬТАТИ РОБОТИ

У дисертаційній роботі вирішено важливу науково-технічну проблему створення і наукового обґрунтування комплексної методології управління процесом обслуговування у інформаційно-комунікаційній мережі мобільного зв’язку з метою підвищення рівня захищеності та якості зберігання, обробки й передачі даних.

За підсумками вирішення проблеми можна зробити наступні висновки:

1. Проведений аналіз особливостей та наявної якості передачі трафіка в 5G мережі та можливих загроз дозволив виявити основні проблеми, такі як зростання обсягів та поява нових джерел трафіка, поява нових вразливостей під час реалізації новітніх сервісів та послуг, що призводить до суттєвого погіршення якості та захищеності процесів надання послуг через відсутність

комплексної методології підвищення захищеності та якості передачі даних в мобільній мережі в цілому.

2. Запропоновано комплексну методологію підвищення захищеності та якості передачі даних в мобільній 5G мережі, яка відрізняється багатокритеріальною оптимізацією за критеріями якості та захищеності, де підвищення захищеності досягається за рахунок застосування інтелектуальної системи управління, нового методу формування ключа з біометричних ознак користувача, вдосконаленого протоколу обміну повідомленнями, запропонованої системи управління приватними даними користувача, що в цілому дозволяє покращити показники конфіденційності, цілісності, доступності та спостереженості; підвищення якості досягається впровадженням методу розподілу навантаження для граничних обчислень з множинним доступом, новітніх методів класифікації трафіка та методів завадостійкого кодування, що в цілому дозволяє покращити показники ймовірності помилки, рівня втрат пакетів, швидкості обробки пакетів, а також пропускної здатності.

3. Вдосконалено модель аналізу та обробки даних у вузлі мережі шляхом застосування методів та технік нечіткої логіки та машинного навчання для попереднього очищення даних від випадкових помилок, множини правил нечіткої бази знань від дублікатів та конфліктів, а також візуалізації за допомогою метаграфу, що дозволяє покращити показники якості класифікації даних у вузлах мережі, пришвидшити обробку трафіка, виявляти аномалії у трафіку під час забезпечення захисту мережі.

4. Вдосконалено набір ознак для класифікація трафіка за критеріями складності і швидкодії шляхом зменшення їх кількості без суттєвої втрати точності, а саме: зменшення набору ознак з 82 до 56 (на 31.7%), що підвищило швидкість процедури класифікації на 3.4%.

5. Визначено найкращі методи машинного навчання (Random Forest, Decision Tree) для класифікації трафіка у вузлі мережі та їх гіперпараметри, які обираються інтелектуальною системою динамічно. Найвища продуктивність при прийнятній точності досягається при розмірі виборки 128, кількості епох 10 та використанні малого (18) або середнього (54) набору ознак. Запропоновані гіперпараметри та методи є першим етапом багатокрокової обробки пакетів в мережі, що разом з кластеризацією, слайсінгом та розподіленою обробкою дозволять підвищити ефективність системи мобільного зв’язку в цілому.

6. Вдосконалено метод розподілу навантаження для граничних обчислень з множинним доступом (MEC), новизна якого полягає в інтелектуальному розподілі даних MEC, додаванні надмірності під час розподілу (паралелізації обчислень), додаванні функції контролю помилок і оцінюванні ефективності кожного вузла обчислень шляхом присвоєння рівня довіри, що дозволяє мінімізувати ймовірність помилки розрахунків та обсяг використаних ресурсів мережі під часу розподілу завдань граничних обчислень.

7. Вдосконалено метод завадостійкого кодування пакетів під час їх передачі мобільною мережею шляхом реалізації: нового методу формування коду Raptor з міжблоковою схемою перемежіння. Запропоновані модифікації коду дозволяють зменшити рівень втрат пакетів до 11% в каналах із затираннями.

8. Вдосконалено метод формування вектору ознак біометричних характеристик користувача шляхом реалізації нового модуля агрегації; визначення пріоритетів біометричних ознак; зашумлення невикористовуваних ознак; проріджування; завадостійкого кодування та врахування стану каналу зв'язку, що дозволило підвищити рівень послуг конфіденційності та спостереженості.

9. Вдосконалено процес підготовки біометричних даних користувача до передачі мережею зв'язку шляхом підвищення порогу спрацьовування системи у зашумлених каналах зв'язку і приховування сеансу віддаленої автентифікації в заголовках мережних протоколів, що дозволяє на 10% зменшити рівень помилок FRR і підвищити рівень спостереженості.

10. Вперше запропоновано метод взаємної автентифікації користувачів під час дзвінка, шляхом модифікації полів повідомлень SETUP, CONNECT ACK та застосуванням різних видів біометричної автентифікації (в залежності від сценарію), що дозволяє уникнути підміни користувача на іншому боці, отримати доступ до сервісів лише авторизованому користувачу і підвищити рівні послуг конфіденційності, цілісності та спостереженості.

11. Підвищено рівень послуг конфіденційності й цілісності під час розмови по мобільній мережі шляхом застосування: протоколу Діффі-Хелмана для безпечного обміну ключами; короткого автентифікаційного рядка для протидії атаці "зловмисник-посередині"; хешу попереднього дзвінка для протидії спуфінгу телефонних номерів; симетричного шифрування мови алгоритмом AES(256) для протидії прослуховуванню і підвищення рівня конфіденційності при обміні. Для реалізації протоколу обміну ключами Діффі-Хелмана запропоновано модифікацію повідомлень SETUP і CONNECT в традиційній послідовності під час встановлення дзвінка.

12. Розроблено нові моделі управління приватними даними користувача для забезпечення захищеності даних під час реалізації нових сервісів, що дозволяють надавати користувачу додаткові можливості без зниження рівня захищеності. Перший метод пропонує використання біометричної автентифікації, машинного навчання та розпізнавання зображень для надання користувачу можливості віддаленого управління об'єктами. Другий – зберігання приватних даних користувача в захищеному ієрархічному вигляді і доступ до них різного рівня у надзвичайних випадках. Запропоновані рішення запатентовані і впроваджені в обладнанні Samsung.

13. Виконано оцінку ефективності запропонованих рішень. Результати апробації показали зменшення рівня втрат пакетів на 11%, зменшення затримки на обробку трафіка і вдосконалення рівня послуг із захищеності на 29%.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у фахових виданнях України, які включені до міжнародних наукометричних баз (Scopus)

1. Astrakhantsev A., Liashenko, G. “Data protection management process during remote biometric authentication”, System Research and Information Technologies, №3 2022, pp. 71–85. **(Scopus)**

2. Astrakhantsev A., Pedan S. “Improving user security during a call”, Radioelectronic and Computer Systems, 2024, no. 2(110), pp.173-185. **(Scopus)**

3. Astrakhantsev A., Globa L., Fedorov O., Romanko Y. “An improved approach to organizing mobile edge computing in a 5G network”, System Research & Information Technologies, 2024, No 2, pp. 82-92.

Статті у наукових фахових виданнях України:

4. Астраханцев А.А., Волотка В.С., Семашко Е.М. “Захист інформації в системах мобільного зв’язку за допомогою гамування” [рос], Східно-Європейський журнал передових технологій. – 2009. – №4/3 (40). – С. 20-23.

5. Астраханцев А.А., Войтюк А.А. “Аналіз ефективності і завадостійкості системи OFDM”, Східно-Європейський журнал передових технологій. – 2011. – №3/9 (51). – С. 21-23.

6. Астраханцев А.А., Дорожан А.В., Вовк О.О. “Дослідження характеристик методів приховування з використанням НЗБ на тлі адитивного шуму”, Вісник НТУ «ХПІ». – 2012. – №18. – С. 37-40.

7. Астраханцев А.А., Дорожан А.В., Вовк О.О. “Дослідження стійкості методів приховування інформації в нерухомих зображеннях” [рос], Системи обробки інформації. – Х.: ХУПС – 2012. – №2. – С. 104-109.

8. Астраханцев А.А., Новіков Р.С. “Аналіз характеристик завадостійких кодів” [рос], Системи обробки інформації. – Х.: ХУПС – 2013. – №9 (116) – С. 164-167.

9. Астраханцев А.А., Новіков Р.С. “Вибір параметрів LDPC кодів для каналів з АБГШ” [рос], Системи обробки інформації. – Х.: ХУПС – 2014. – №1 (117). – С. 195-199.

10. Астраханцев А.А., Вовк О.О. “Розробка методики та оцінювання важливості характеристик стеганографічних алгоритмів”, Вісник національного університету Львівська Політехніка «Інформаційні системи та мережі. Львів, 2014. – № 805. – С. 52-60.

11. Астраханцев А.А., Вовк О.О. “Аналіз ефективності застосування вейвлет-перетворення в стеганографічних системах передавання даних”, Вісник національного університету Львівська Політехніка «Інформаційні системи та мережі. Львів, 2015. – № 832. – С. 9-17.

12. Астраханцев А.А., Вовк О.О. “Синтез методу прихованої передачі інформації, ефективного за критеріями надійності та захищеності”, Проблеми телекомунікацій. – Х.: ХНУРЕ. – 2015. – №1. – С. 103-115.

13. Астраханцев А.А., Шостак Н.В., Романько С.В. “Дослідження стійкості авторських прав на відеопродукцію”, Системи обробки інформації. – Х.: ХУПС – 2017. – №2 (148). – С. 138-143.

14. Астраханцев А.А., Ляшенко Г.Є. “Дослідження ефективності методів біометричної автентифікації”, Системи обробки інформації. – Х.: ХУПС – 2017. – №2 (148). – С. 111-114.

15. Астраханцев А.А., Щербак А.О., Щербак О.В. “Аналіз скритності та стійкості до шуму в каналах зв’язку методів мережної стеганографії”, Проблеми телекомунікацій. – Х.: ХНУРЕ. – 2018. – №2. – С. 89-98.

16. Астраханцев А.А., Шостак Н.В., Безрук В.М. “Вибір переважного алгоритму вбудовування цифрових водяних знаків в відеофайли”, Радіоелектроніка, інформатика, управління. – Запоріжжя, ЗНТУ. – 2018. – №3(46). – С. 167-173.

17. Астраханцев А.А., Чєрнікова В.Г., Ляшенко Г.Є. “Дослідження характеристик системи біометричної ідентифікації по райдужній оболонці ока”, Системи озброєння і військова техніка. – 2018. – №1. – С. 195-202.

18. Астраханцев А.А., Шостак Н.В. “Аналіз стійкості стеганографічних методів вбудовування даних в відеофайли до атак”, Системи обробки інформації. – Х.: ХУПС – 2019. – №3. – С. 110-116.

19. Astrakhantsev A., Ostapenko M., Shtogrina O., Globa L. “Developing a computer vision re-identification system”, Information and Telecommunication Sciences. – 2020. – №1. – P. 35-40.

20. Astrakhantsev A., Liashenko G., Shcherbak A. “Noise resistance of remote authentication via LTE network”, Information and Telecommunication Sciences. – 2020. – №2. – P. 38-43.

21. Astrakhantsev A., Davydiuk A. “Improved cluster management method for industrial “Internet of Things” network”, Information and Telecommunication Sciences. – 2020. – №2. – P. 81-85.

22. Астраханцев А.А., А.О. Щербак, О.В. Щербак, Г.Є. Ляшенко. “Дослідження завадостійкості біометричних шаблонів до зовнішніх впливів під час передачі мобільними мережами”, Проблеми телекомунікацій. – 2020. – №1 (26). – С. 63-72.

23. Астраханцев А.А., Л.С. Глоба, А.М. Давідюк, О.В. Сушко. “Дослідження ефективності алгоритмів машинного навчання для класифікації трафіка в мобільних мережах”, Проблеми телекомунікацій. – 2022. – №1 (30). – С. 3-17.

24. Астраханцев А.А. Г.Є. Ляшенко. “Процес керування захищеністю даних під час віддаленої біометричної автентифікації”, System research and information technologies. – 2022. – №3. – С. 71-85.

25. Astrakhantsev A., Globa L., Sushko O., Davydiuk A. “Adjusting the parameters of machine learning algorithms to improve the accuracy of traffic classification”, Information and Telecommunication Sciences. – 2023. – P. 26-32.

26. Астраханцев А. Глоба Л., Цуканов С. “Класифікація мережевого трафіку методами машинного навчання”, Проблеми телекомунікацій. – 2023. – №2. – С. 3-13.

27. Astrakhantsev A., Leliak A. “Improve mobile driving license data transfer security via BLE/Wi-Fi aware with UWB ranging”, Problemi Telekomunikacij. – 2023. – №2 (33) – С. 62-74.

28. Astrakhantsev A., Hryschuk I., Pedan S., Globa L. “Analysis of routing protocols characteristics in ad-hoc network”, Information and Telecommunication Sciences. – 2024. – №1 – P. 12-17.

Статті у виданнях інших держав та додаткова література:

29. Astrakhantsev A., Dorozhan A. “Research methods for improving noise immunity of secure data transmission”, Science Publishing Group. – №1(4), New York, USA, 2013. – pp. 28-36.

30. Astrakhantsev A., Vovk O. “Synthesis of optimal steganographic method meeting given criteria”, Informatyka Automatyka Pomiary w Gospodarce i Ochronie Środowiska (technical and scientific journal), Lublin, Poland, 2015. – pp. 27-34.

31. Astrakhantsev A., Shostak N., Romanko S. “Comparative analysis of effectiveness video watermarking techniques”, Global Science Center LP. – Sciences of Europe (Praha, Czech Republic) # 15-1 (15), 2017. – pp. 92-95.

32. Інформаційні мережі зв’язку. Т. 2. Телекомунікаційні технології стаціонарних мереж зв’язку [Текст]: навч. посібник // упорядники: Безрук В.М., Бідний Ю.М., Астраханцев А.А., Колтун Ю.М. – Х.: ХНУРЕ. – 2011. – 502с.

33. Інформаційні мережі зв’язку. Т. 4. Технології надання інформаційних послуг [Текст]: навч. посібник // упорядники: Безрук В.М., Корольов В.М., Золотарьов В.А., Астраханцев А.А. – Х.: ХНУРЕ. – 2011. – 424с.

34. Астраханцев А.А., Безрук В.М. Маршрутизація в мережах зв’язку [Текст]: навч. посібник з грифом МОНУ – Х.: ТОВ «Компанія СМІТ». – 2011. – 368с.

Патенти та авторські свідоцтва:

35. Sun-Kyung Kim, Astrakhantsev A., Yakishyn Y., Korobov M. “System and method for providing information using near field communication”, US Patent App. US15/781,636, 2020 (US10986462B2)

36. Astrakhantsev A., Shchur O., Korobov M., Oliynyk A., Jae-Hong Kim “Electronic device and method for providing user information”, US Patent App. US15/778,818, 2018 (EP3367277A1).

37. Popov A., Popov O., Astrakhantsev A., Pedan S., Shapoval I., Konoval O. “Electronic device and method of operating the same”, US Patent App. US18/163,589 (US20230259652A1).

38. Popov A., Popov O., Kulakov A., Astrakhantsev A., Shchur O., Tatarinova Y. “Method for securing image and electronic device performing same”, US Patent App. US17/378,032, 2021 (US20210342967A1).

39. Pedan S., Kopysov O., Popov O., Chalyi O., Astrakhantsev A. “Folderable devices and methods of operation thereof”, Korean patent KR20220007352.

40. Progonov D., Popov O., Astrakhantsev A., Motchanyi A. “Device and method for acquiring biosignal”, WO2024096391A1.

41. Авторське право на твір №116973 від 10.03.2023: Науковий твір «Силабус навчальної дисципліни «EU5G4UA: Застосування інструментарію та фреймворків ЄС для мереж 5G для України (EU5G4UA: Application of EU toolbox and frameworks of 5G networks for Ukraine)» // Турута О.П., Турута О.В., Астраханцев А.А., Євдокименко М.О., Даніель Я.Д.

Матеріали та тези наукових конференцій, які індексуються у Scopus:

42. Astrakhantsev A., Globa L., Astrakhantsev O. “Computational Intelligence for Voice Call Security: Encryption and Mutual User Authentication”, Digital Ecosystems: Interconnecting Advanced Networks with AI Applications. TCSET 2024. Lecture Notes in Electrical Engineering, vol 1198. Springer, Cham. pp. 714-733. **(Scopus)**

43. Astrakhantsev A., Doroghan, O., Poponin, O., Shostak, N. “Studying of stability of the information hiding methods in still images”, Modern Problems of Radio Engineering, Telecommunications and Computer Science – Proceedings of the 11th International Conference, TCSET'2012. – P. 409. **(Scopus)**

44. Astrakhantsev A., Liashenko G., Chernikova V. “Network steganography application for remote biometrie user authentication”, Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018. – pp. 326-330. **(Scopus)**

45. Astrakhantsev A., Liashenko G. “Investigation of the influence of image quality on the work of biometric authentication methods”, 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 – Proceedings. – pp. 543-546. **(Scopus)**

46. Astrakhantsev A., Shcherbak A., Shcherbak O., Liashenko G. “Biometric templates noise immunity during transmission by mobile networks”, CEUR Workshop Proceedings, 2021, 2923, pp. 175–181. **(Scopus)**

47. Astrakhantsev A., Globa L, Novogrudska R, Skulysh M, Stryzhak O. “Improving resource allocation system for 5G networks”, 2021 International Conference on Information and Digital Technologies (IDT) – 2021. – pp. 182-188. **(Scopus)**

48. A. Astrakhantsev, L. Globa, A. Davydiuk and O. Sushko, "Feature Set Optimization for Machine Learning Traffic Classification in Mobile Networks," 2023 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Istanbul, Turkiye, 2023, pp. 369-370, **(Scopus).**

49. Astrakhantsev A., Globa L., Pedan S., Mysko N. “Secured method of providing hierarchical private data via a smartphone”, IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics – 2023. – pp.50-53. **(Scopus)**

50. Astrakhantsev A., Globa L., Tsukanov S. “Approach to Traffic Classification in 5G Networks”, 2024 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Tbilisi, Georgia, 2024, pp. 332-336. **(Scopus)**

51. Astrakhantsev A., Liashenko G. “Implementation biometric data security in remote authentication systems via network steganography”, Advances in Information and Communication Technology and Systems: Lecture Notes in Networks and Systems, Springer International Publishing 2021, 152, pp. 257–273. **(Scopus)**

Матеріали та тези міжнародних наукових конференцій:

52. Астраханцев А.А., Вакуленко В.С. “Підвищення ефективності алгоритмів приховування інформації в нерухомих зображеннях” [рос], 1-а Міжнародна конференція «Безпека та захист інформації в інформаційних та телекомунікаційних системах». – Х.: ХНЕУ, 2008. – С. 27-28.

53. Астраханцев А.А., Бондар І.В. “Конфіденційність і захист в мережах стандарту GSM. Пакетна передача даних в з розробкою механізмів захисту трафіка”

[рос], 1-а Міжнародна конференція «Безпека та захист інформації в інформаційних та телекомунікаційних системах». – Х.: ХНЕУ, 2008. – С. 20-21.

54. Астраханцев А.А., Катюшина О.Р. ”Підвищення стійкості алгоритмів захисту мови в мережах мобільного зв’язку” [рос], 13-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2009. Т.2 – С. 62.

55. Астраханцев А.А., Варич В.В. “Керування трафіком і забезпечення якості обслуговування в IP-мережах” [рос], 13-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2009. Т.1 – С. 197.

56. Астраханцев А.А., Вакуленко В.С. “Дослідження методів підвищення надійності стеганосистем” [рос], 13-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2009. Т.2 – С. 60.

57. Астраханцев А.А., Гулякова Т.Б. “Аналіз якості мови в корпоративних мережах супутникового зв’язку” [рос], 13-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2009. Т.1 – С. 194.

58. Астраханцев А.А., Бєлікова І.В. “Дослідження захищеності електронних платежів в корпоративних мережах” [рос], 14-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2010. Т.1 – С. 225.

59. Астраханцев А.А., Краснянський В.В. “Аналіз характеристик корпоративних супутникових мереж зв’язку” [рос], 14-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2010. Т.1 – С. 228.

60. Астраханцев А.А., Копитова М.О. “Аналіз якості та захищеності мови в мережі IP-телефонії”, 14-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті».– Х.: ХНУРЕ. – 2010. Т.1 – С. 244.

61. Астраханцев А.А., Кузнєцова Є.О. “Дослідження характеристик стеганографічних систем передачі інформації”, 14-й Міжнародний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2010. Т.1 – С. 192

62. Астраханцев А.А., Лесковець Л.І. “Застосування ймовірнісного підходу для побудови систем захисту інформації в мережах зв’язку”, 14-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2010. Т.1 – С. 200.

63. Астраханцев А.А., Шостак О.В. “Дослідження методів забезпечення якості у IP-мережах”, 14-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті».– Х.: ХНУРЕ. – 2010. Т.1 – С. 209.

64. Астраханцев А.А., Афанасьєвський Ю.В. “Аналіз характеристик систем електронної ідентифікації на основі систем RFID” [рос], 15-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2011. Т.4 – С. 140.

65. Астраханцев А.А., Войтюк А.А. “Дослідження завадозахищеності та ефективності в бездротових мережах з OFDM модуляцією”, 15-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2011. Т.4 – С. 158.

66. Астраханцев А.А., Вовк О.О. “Дослідження стійкості цифрових водяних знаків у відеофайлах і зображеннях”, 15-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2011. Т.4 – С. 156.

67. Астраханцев А.А., Шостак О.В. “Аналіз методів керування трафіком у мультисервісній мережі”, 15-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті».– Х.: ХНУРЕ. – 2011. Т.4 – С. 208.

68. Астраханцев А.А., Дорожан А.В. “Дослідження стійкості стеганосистем” [рос], Інфокомунікації – сучасність та майбутнє: матеріали першої міжнар. наук.-пр. конф. молодих вчених. – Одеса: ОНАЗ. – 2011. – Ч.1, С.118-120.

69. Астраханцев А.А., Войтюк А.А. “Дослідження завадостійкості алгоритмів модуляції OFDM та DMT”, Інфокомунікації – сучасність та майбутнє: матеріали першої міжнар. наук.-пр. конф. молодих вчених. – Одеса: ОНАЗ. – 2011. – Ч.1, С.109-111.

70. Астраханцев А.А., Вовк О.О. “Дослідження та порівняльна характеристика методів вбудовування інформації для прихованої передачі у мережах зв’язку”, Інфокомунікації – сучасність та майбутнє: матеріали першої міжнар. наук.-пр. конф. молодих вчених. – Одеса: ОНАЗ. – 2011. – Ч.1, С.105-108.

71. Астраханцев А.А., Романько С.В., Шостак Н.В. “Дослідження стійкості до атак алгоритмів захисту авторських прав на відеопродукцію”, Міжнародна науково-практична конференція «Проблеми і перспективи розвитку ІТ- індустрії». – Х. – 2017. – С. 64.

72. Астраханцев А.А., Щирова Ю.А. “Багатокритеріальний аналіз ефективності систем автентифікації користувача”, 21-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2017. – Т.4 – С. 136-137.

73. Астраханцев А.А., Жмакіна В.В. “Порівняльний аналіз протоколів мультикаст доставки контенту в мережі IPTV”, 21-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2017. – Т.4 – С. 155-156.

74. Астраханцев А.А., Чернікова В.Г., Стрілець А.М. “Дослідження характеристик системи біометричної ідентифікації по радужній оболонці ока”, 21-й Міжнародний Молодіжний Форум «Радіоелектроніка та молодь в XXI столітті». – Х.: ХНУРЕ. – 2017. – Т.4 – С. 44-45.

75. Астраханцев А.А., Форостянко К.Ю. “Efficiency of user authentication methods in mobile networks”, 17-а міжнародна науково-технічна конференція "Перспективи телекомунікацій". – К.: НТУ КПІ. – 2023. – pp. 229-232.

76. Астраханцев А.А., Сушко О.В. “Study of the efficiency of machine learning algorithms for traffic classification in mobile networks”, 17-а міжнародна науково-технічна конференція "Перспективи телекомунікацій". – К.: НТУ КПІ. – 2023. – pp. 232-235.

АНОТАЦІЯ

Астраханцев А. А. **Моделі та методи підвищення захищеності та якості передачі даних в системах мобільного зв’язку**. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі. – Національний

технічний університет України "Київський політехнічний інститут ім. Ігоря Сікорського" Міністерства освіти і науки України, м. Київ, 2024.

Дисертаційна робота присвячена вирішенню актуальної наукової проблеми створення і наукового обґрунтування комплексної методології управління процесом обслуговування у інформаційно-телекомунікаційній мережі мобільного зв'язку з метою підвищення рівня захищеності та якості процесу обслуговування користувачів. Розроблено та досліджено моделі та методи попередньої обробки трафіка у вузлі мережі, включаючи алгоритми підготовки даних, класифікації та кластерізації трафіка. Для розподілених граничних обчислень (МЕС) запропоновано метод організації обчислень, розподілення і контроля навантаження та перевірки результатів. Проведено розробку та вдосконалення моделей та методів завадостійкого кодування в мобільних мережах шляхом вдосконалення методу формування коду Raptor. Проведено вдосконалення обробки даних у пристроях користувача направлені на підвищення захищеності приватних даних і перекриття типових атак пов'язаних з підміною користувачів. Для цього в дисертації запропоновані і досліджені методи формування біометричного шаблону користувача, методи його прихованої передачі, методи взаємної автентифікації та шифрування під час голосового дзвінка. Розроблено і впроваджено методи управління приватними даними користувача на мобільному пристрої.

На основі отриманих результатів запропоновано інтелектуальну систему управління, що забезпечує оптимізацію за обраними критеріями методу класифікації трафіка, врахування параметрів каналу зв'язку для вибору алгоритмів кодування і модуляції, а також вибір методів захисту приватних даних користувача, включаючи вибір методу стеганографічного приховування даних.

Ключові слова: управління мобільними мережами, розподілені граничні обчислення, класифікація та кластеризація трафіка, набір ознак, нейронні мережі, завадостійке кодування, фонтанні коди, управління захищеністю даних, конфіденційність даних, захист від атак, взаємна автентифікація користувачів під час дзвінка, наскрізне шифрування під час дзвінка, мережна стеганографія.

SUMMARY

Astrakhantsev A. A. Models and methods for improving the security and quality of data transmission in mobile communication systems. – Manuscript. Dissertation for the Doctor of Technical Sciences degree in the specialty 05.12.02 – Telecommunication systems and networks – National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, 2024.

The dissertation is devoted to solving the urgent scientific problem of creating and scientific substantiation of a comprehensive methodology for managing the service process in an information and telecommunication network of mobile communications in order to increase the level of security and quality of the user

service process. Models and methods of traffic pre-processing in a network node, including algorithms for data preparation, classification and clustering of traffic, were developed and investigated. For mobile edge computing, a method for organizing computations, distributing and controlling the load, and verifying the results is proposed. The models and methods of noise-resistant coding in mobile networks are developed by improving the method of Raptor code formation.

Improvements in data processing in user devices are aimed at increasing the security of private data. For this purpose, the thesis proposes and investigates methods for generating a user's biometric template, methods for its covert transmission, methods of mutual authentication and encryption during a voice call. Methods for managing user's private data on a mobile device are developed and implemented.

Keywords: mobile network management, distributed edge computing, traffic classification and clustering, feature set, neural networks, noise-resistant coding, fountain codes, data security management, data privacy, attack protection, mutual user authentication during a call, end-to-end encryption during a call, network steganography.