Хмельницький національний університет
Факультет програмування
та комп'ютерних і телекомунікаційних систем
Кафедра комп'ютерної інженерії та системного програмування

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Засоби сенсорного зв'язку критичних за часом хмарних обчислень
Назва теми

КвРКІ.170157.17.01.24 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія»*
Назва

Виконав: студент IV курсу, група КІ–17–2 _____ Д.О. Островський
Підпис Ініціали, прізвище

Керівник _____ О.С. Савенко
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ С.М. Лисенко
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри комп'ютерної
Інженерії та системного
Програмування _____ Т.О. Говорущенко
Підпис Ініціали, прізвище

«____» _червня_ 2021 р.

Хмельницький 2021

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Програмування та комп'ютерних і телекомунікаційних систем

Кафедра Комп'ютерної інженерії та системного програмування

Освітній рівень бакалавр

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Зав. кафедри Т.О.Говорущенко

"11" 01 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Островський Денис Олексійович

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Засоби сенсорного зв'язку критичних за часом хмарних обчислень

Керівник проекту (роботи) Савенко О.С., д.т.н., проф.

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 05.02.2021 р. № 11

2. Строк подання студентом проекту (роботи) на кафедру 07.06.2021 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Дослідження предметної області та постановка задачі

Проектування засобів сенсорного зв'язку критичних за часом хмарних обчислень

Програмно-апаратна реалізація та тестування засобів сенсорного зв'язку критичних за часом хмарних обчислень

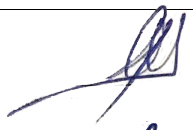
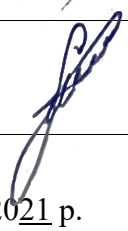
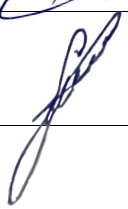
5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Детермінована інтерпретація кінцевих автоматів для кожного обмеження

П'ятифазний сценарій DDoS-атаки

Глобальний автомат для трьох обмежень

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Лисенко С.М., професор кафедри КІСП		
Антиплагіат	Нічепорук А.О., доцент кафедри КІСП		

7. Дата видачі завдання «_11_»_____01_____2021 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	11.01.2021	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об’єкта та предмета дослідження	01.02.2021	виконано
3	Робота над розділом 1 – дослідження предметної області та постановка задачі	01.03.2021	виконано
4	Робота над розділом 2 – моделювання та проєктування засобів зв’язку	01.04.2021	виконано
5	Робота над розділом 3 – програмно - апаратна реалізація мультипроцесорної системи	30.04.2021	виконано
6	Оформлення пояснювальної записки згідно вимог	31.05.2021	виконано
7	Попередній захист ВКР	02.06.2021	виконано
8	Захист ВКР на засіданні ЕК	Червень 2021 року	

Студент _____ Підпис _____Д.О. Островський_____ Ініціали, прізвище

Керівник проекту (роботи) _____ Підпис _____О. С. Савенко_____ Ініціали, прізвище

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ 170157.17.01.24 ПЗ	Пояснювальна записка	80		
			Графічні матеріали			
2		КвРКІ 170157.17.01.24 Е8	Детермінована інтерпретація кінцевих автоматів для кожного обмеження	1		
3		КвРКІ 170157.17.01.24 Е8	П’ятифазний сценарій DDoS-атаки	1		
4		КвРКІ 170157.17.01.24 Е8	Глобальний автомат для трьох обмежень	1		

Зм	Арк	№ докум	Підпис	Дата	КвРКІ 170157.17.01.24 ВП			
Розробив		Островський			Відомість проекту	Літера	Аркуш	Аркушів
Перевір.		Савенко				У	1	1
Н. контр.		Лисенко				ХНУ, КІ-17-2		
Затв.		Говорущенко						

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Засоби сенсорного зв’язку критичних за часом хмарних обчислень».

Автор роботи: Островський Денис Олексійович.

Керівник роботи: Савенко Олег Станіславович.

Пояснювальна записка: 80 с., 13 рис., 7 табл., 4 дод., 50 джерел.

Графічна частина: 10 презентаційних слайдів.

ЗАСОБИ СЕНСОРНОГО ЗВ’ЯЗКУ КРИТИЧНИХ ЗА ЧАСОМ ХМАРНИХ ОБЧИСЛЕНЬ

Метою роботи є розробка засобів сенсорного зв’язку критичних за часом хмарних обчислень.

Основним внеском цієї дипломної роботи є нова метрика довіри для відбору не зловмисних Кооперативні користувачі зондування спектра для надійного виявлення вакантних каналів, надійний метод управління передачею когнітивного радіоспектру, чутливий до затримки, для безшовної зв’язки та енергозберігаючий спосіб розбору ключа шифрування на основі функції шифрування на основі функції для безпечної передачі даних. Крім того, розроблений метод вибору постачальника ідентифікаційних даних на основі довіри для аутентифікації користувачів та надійний конкретний метод авторизації, що відповідає конкретній ситуації, розроблений для більш надійного та безпечного доступу до дати у хмарних сховищах. На закінчення, ці внески можуть цілісно сприяти пом'якшенню вищезазначених умов відмови для досягнення передбачуваної надійності критично важливих для часу програм віддаленого моніторингу.

Підпис студента Дата

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

БМД - багатоатрибутна метрика довіри

ПК - первинний користувач

ВК - вторинний користувач

КР - когнітивне радіо

МКР - мережа когнітивного радіо

СМКР - сенсорна мережа когнітивного радіо

ФДЗС - фальсифікація даних зондування спектру

ПХП - постачальник хмарних послуг

ЦС - центр синтезу

ВСТУП

Хмарні технології сьогодення охоплюють велику частину ринку в IT, в деяких країнах понад 50% всіх організацій працює саме в хмарних сервісах. Пезперебійність та надійність цих систем має надзвичайно велику вагу у сучасному світі. Критично важливі для часу системи дистанційного моніторингу (TCRMS) збирають великі обсяги даних за допомогою датчиків та агрегаторів даних. За допомогою даних віддаленого моніторингу приймаються критично важливі для часу рішення. Приклади TCRMS включають моніторинг критичних компонентів інтелектуальної мережі, програми телемоніторингу у всепроникній охороні здоров'я, дистанційний контроль стану силових установок, системи управління будівлею рішення для домашнього догляду за літніми людьми та навколишнє середовище.

Актуальність роботи полягає в застосуванні найдійних засобів сенсорного зв'язку критичних за часом хмарних обчислень.

Метою кваліфікаційної роботи є розробка засобів сенсорного зв'язку критичних за часом хмарних обчислень.

Досягнути поставлену мету можна розв'язанням наступних основних задач:

1) необхідно провести дослідження вже наявних рішень, для визначення вимог та правил побудови мультипроцесорних систем;

2) виконати дослідження наявних проблем та обмежень існуючих рішень розробки та шляхи їх рішення;

3) розробити метод створення засобів;

4) розробити алгоритм та імплементувати деякі його аспекти для засобів зв'язку критичних за часом хмарних обчислень.

1 НАДІЙНА ПЕРЕДАЧА ДАНИХ ЧЕРЕЗ СМКР НА ОСНОВІ БАГАТОАТРИБУТНИХ ДОВІР

1.1 Багатоатрибутна метрика довіри

У цьому розділі виведено запропоновану багатоатрибутну метрику довіри та проаналізовано надійність метрики. Передбачається, що рішення про централізовану доступність спектра приймаються в центрі термоядерного синтезу (ЦС) шляхом комбінування місцевих рішень довірених кооперативних користувачів відповідно до наборів заздалегідь визначених правил [1][2][3][4]

1.2 Атрибути довіри

Довіра - це, по суті, багатовимірна риса, яка може бути описана набором атрибутів, що відповідають кожному з обраних вимірів. Для обчислення багатовимірної довіри необхідні кілька атрибутів [5][6][7]. Після того, як визначено кілька атрибутів, потрібно обчислити функціональну форму комбінації цих атрибутів. У [9], атрибут визначається як розмірний простір. Атрибут може приймати значення в цьому розмірному просторі. Використовуючи багатоатрибутну теорію корисності [10][11], виходячи із залежностей між цими атрибутами, виведено відповідну функціональну форму.

Запропонована багатоатрибутна метрика довіри складається з трьох атрибутів A1, A2, A3 що відповідає трьом вимірам. Ці три виміри характеризують надійність. Сутність ВК полягає в наступному:

1) ВК надає точні рішення щодо зондування для ЦС за запитом;
2) ВК відповідає місцевими рішеннями зондування;
3) ВК справді вимагає доступу до спектру для передачі даних.

Для визначення прямої довіри кооперативної ВК, перший атрибут довіри (A1) обчислюється на основі ймовірності фальсифікації даних зондування спектру

протягом часу "t", використовуючи раніше виявлені такі неправильні дані протягом фіксованого часового вікна.

$$A_1 = \frac{X_j}{X_{заг,j}}, \quad (1.1)$$

де Xj позначає кількість випадків, коли дані зондування спектру були хибними і Xtotal, j представляє загальну кількість коректних даних зондування спектру, надісланих j-ю ВК протягом фіксованої тривалості часу. Більше значення A1 відображає більшу надійність. Можливі значення A1 включають максимум 1 і мінімум 0. Передбачається, що кооперативний ВК використовує техніку детектування енергії для виявлення ПК [12]. Значення Xj та Xtotal, j можна обчислити, використовуючи дані історії взаємодії, що зберігаються у ФК. Рішення про доступність спектра визначається на основі заздалегідь визначеного порогу для методу виявлення енергії [12]. У ФК також передбачається, що на основі загального рішення кожні окремі дані локального зондування спектру класифікуються як правильні або помилкові дані зондування.

Далі вибирається другий атрибут A2, який характеризує чуйність ВК. Передбачається, що коли запит ЦС на дані локального зондування, реагуючий ВК надсилає результат зондування спектру. Передбачається, що ВК має хороший прийом каналу управління для прийому запиту від ЦС. Невідповідь розглядається як вказівка на ненадійного користувача.

$$A_2 = \frac{D_{rsp,\,j}}{Resp_j}, \quad (1.2)$$

де D_{rsp}, j і $Resp_j$ позначають кількість відповідей, отриманих від j-го ВК і загальну кількість запитів зондування спектру, отриманих j-м ВК відповідно. Що більше значення A2, то надійність висока. Можливі значення A2 включають максимум 1 і мінімум 0. Передбачається, що комунікації з точки зору відповідей та

запитів записуються у вигляді матриці записів відповідей на ЦС. Рядки та стовпці матриці відповідають відповідям та запитам.

Далі, третій атрибут довіри (А3) обчислюється на основі історії запитів доступу до каналу. Коли ВК вказує на вимогу передавати дані, для ВК визначається канал, якщо він є вакантним в момент часу t. Термін відносна жадібність використовується для характеристики ВК для використання більшої кількості ресурсів спектра для передачі на основі швидкості розподілу спектру. Передбачається, що коли деякі ВК не отримують можливості передавати в певному часовому інтервалі, вони мають більший попит на передачу в наступний часовий інтервал. Така наполеглива поведінка при доступі до каналу характеризується як жадібність.

$$A_З = \frac{I_j}{I_{уяв}}, \tag{1.3}$$

де lI_j представляють ступінь жадібності, а $I_{уяв}$ - середній ступінь жадібності протягом певного періоду часу. Для обчислення значення I_j враховується середня потужність сигналу протягом цього фіксованого періоду часу T і частота відмов розподілу каналів. Це еквівалентно розрахунку поточної довіри з використанням фактора забуття (FGF) [13]. Фактор забуття включається для вираження відносної несвіжості відношення середньої сили сигналу протягом фіксованого періоду часу. У [13], як правило, вважається, що FGF = 0,9, що вказує на те, що коефіцієнт не різко змінюється.

$$I_j = FGF \times (\frac{a_j}{r_j}), \tag{1.4}$$

$$I_{уяв.} = \frac{\sum_{j=1}^{K} I_j}{K}, \tag{1.5}$$

де a_j і r_j представляє кількість разів, за які канали були виділені, і дані, передані j-м ВК, і загальну кількість запитів, зроблених цим ВК для доступу до каналу

відповідно. Співвідношення між a_j і r_j являє собою непряму довіру [14] на основі історії розподілу каналів. Значення a_j і r_j обчислюються на основі даних історії розподілу каналів на ЦС для j-го ВК протягом періоду часу T. Значення $I_{уяв.}$ обчислюється як середнє значення I_j для $j = \{1, 2, \cdot \cdot \cdot, K\}$ над T. Чим більше значення A3, тим користувач є надійнішим. Можливі значення A3: max = 1 і min = 0.

На додаток до вищезазначених атрибутів довіри, розглядається також прямий показник довіри, заснований на залишковій енергії кожного ВК. Для ВК, якщо вміст залишкової енергії перевищує заздалегідь визначений поріг, ВК вважається надійним з точки зору експлуатації без збоїв. При виборі довіреного набору для ВК, ця пряма довіра також враховується.

1.3 Функціональна форма багатоатрибутної довіри

Службова програма-функція кількісно визначає перевагу, присвоюючи числове значення для позначення задоволення певного критерію [15]. Відповідно до [16], коли кооперативні користувачі обираються з використанням різних стратегій, утиліти вибір варіюється. Також вплив переваг (тобто, $k_{масшт,i}$ у рівнянні 1.6) серед атрибутів довіри різняться. Далі корисність БМД обчислюється за допомогою багатоатрибутної теорії корисності [17]. Три основні кроки [18] для обчислення значення корисності БМД є (i) визначення функцій корисності для кожного атрибута A1, A2 і A3, (ii) перевірка умов незалежності корисності та (iii) ідентифікація функціональної форми багатоатрибутної утиліти функція для БМД.

Для обчислення функціональної форми БМД використовується багатоатрибутна теорія корисності [19]. Відповідно до [19], описано кілька вимірів метрики використовуючи відповідні атрибути мультиплікативно. Цінностівзяті кожним атрибутом відображають загальну довіру до агента. У рівнянні 1.5, три атрибути довіри A1, A2 і A3 використовуються для вираження множинних вимірів загальної міри довіри БМД.

$$МАТМ = A1 \times A2 \times A3. \quad (1.5)$$

Для того, щоб обчислити функціональну форму утиліти для БМД, необхідно виконати умови, зазначені в [19]:

1) мінімальна кількість атрибутів, необхідних для визначення поняття пільгового незалежного танцювати - Відповідно до [19], для пільгових незалежність для підтвердження, потрібно щонайменше три (03). Отже, вибору A1, A2, A3 було б достатньо;

2) незалежність від корисності A1, A2, A3 для всіх можливих сценаріїв. Існує два основних сценарії: (i) коли достатня потужність сигналу або (ii) коли недостатня потужність сигналу є, щоб отримати запит на співпрацю із зондуванням спектру місцеве рішення. У (i), A1, A2, A3 є корисними незалежний. Ці комунальні послуги тільки залежать за часом (наприклад, о котрій годині ВК отримує, відповідає та коли отримує відповідь.). У (ii) корисність A2 та A3 не є незалежними одна від одної, оскільки відповідь залежить від прийому запиту. З іншого боку, A1 - корисність, незалежна від A2 і A3. Отже, можна зробити висновок, що незалежність корисності серед трьох атрибутів зберігається не у всіх сценаріях;

3) пільгова незалежність A1, A2, A3 для всіх можливих сценаріїв. Будь-який сценарій (i) або (ii) існує на конкретний час. Для тих самих сценаріїв (i) та (ii), описаних вище, перевага для кожного атрибута є незалежною, оскільки не існує умовного відношення переваг між атрибутами відповідно до їхніх окремих обчислень (див. Рівняння 1.1, 1.2, і 1.3).

Відповідно до дотриманих вище умов теорема1 доведена в [19] задовольняється для підтвердження корисності БМД j-го ВК (або $u(МАТМ)_j$) приймає адитивну функціональну форму, зазначену наступним чином (Рівняння 1.6).

$$u(МАТМ)_j = \sum_{i=1}^{3} k_{масшт,i} u(A_i), \quad (1.6)$$

Для кожної функції корисності $u(A_i)$, константу масштабування $k_{масшт,i}$ визначається як $0 < k_{масшт,i} < 1$ така, що $\sum_i k_{масшт.,i} = 1$ [19]. Значення $k_{масшт,i}$, є суб'єктивним, оскільки це залежить від конкретного сценарію. Він обраний як якісне значення, яке представляє найбільше і найменш бажані атрибути для цього конкретного сценарію. Потім описані функції корисності $u(A_i)$ для A1, A2, A3.

1) для A1 варіація корисності вважається лінійно погіршеною (від 1 до 0) як відношення Xj всього, j(у рівнянні 3.1) варіюється від 0 до 1. Корисність - це максимум коли дані не виявляються помилковими принаймні один раз. Оскільки A1 є прямим розрахунком довіри, заснованим на минулій поведінці правдивості відповідей, A1 = 0,5 розглядається як точка, де u (A1) дорівнює 50% [5];

2) для A2 варіація корисності вважається лінійно збільшеною (від 0 до 1) як відношення DRSP, j j (у рівнянні 3.2) варіюється від 0 до 1. Корисність - це максимум, коли ВК відповідає на всі запити, отримані від ФК. Оскільки A2 є прямим обчисленням довіри на основі минулого поведінки реагування, A2 = 0,5 розглядається як точка, де u (A2) становить 50% [5];

3) для A3 варіація корисності вважається сигмовидною функцією, яка має найбільшу корисність, коли умови каналу однаково хороші або кращі на j-му ВК (у порівнянні з ЦС). Передбачається, що ЦС мають добрі умови сигналу для зондування каналу ch, отже, коефіцієнт, наведений у рівнянні3.3 має максимум 1 і мінімум 0. Для простоти вважається, що корисність лінійно змінюється від 0 до 1, коли коефіцієнт (A3) змінюється від 0,5 до 1 відповідно. Також передбачається, що корисність складе 50%, коли A3 = 0,75 [5].

1.4 Набір надійних користувачів для кооперативу зондування

У цьому розділі описано надійність вибору довіреного набору користувачів на основі u(БМД). Довірена коаліція (ТК) (рівняння 1.7) визначається як набір ВК, що беруть участь в кооперативному зондуванні спектру.

$$TC = \text{select}(([u(MATM)_j], NR, T_{thr}) \text{and} (E_{residual,j} \geq E_{th})), \quad (1.7)$$

де j = 1, 2, · · ·, NR - кількість ВК. Функцією вибору є рішення функція внесення. Ця функція призначає j-те ВК як члена ТС, якщо значення корисності більше T_{thr}, що є заздалегідь визначеним пороговим значенням ($T_{thr} \in [0, 1]$), і якщо цей ВК має достатні запаси енергії. $E_{residual,j}$ - кількість залишкової енергії j-ї ВК, і вона повинна бути більшою, ніж мінімум, необхідний (E_{th}) для безпечної передачі. Вплив відбору ТК на спільне зондування спектру Формування рішення. Коли двійкові місцеві рішення (або дані зондування) повідомляються ЦС, застосовуються правила синтезу для отримання рішення про співпрацю [4]. Правила синтезу поєднуютьсямісцеві рішення (або дані зондування) для прийняття спільного рішення у ФК. Для заданих Pd, j та Pf, j узагальнені правила синтезу (див. Рівняння 1.8) стверджують, що оголошується правильне первинне виявлення користувача, якщо статистика рішення перевищує поріг λ. Вибрано правило більшості I, оскільки передбачається, що принаймні деякі користувачі ТК виявили сигнал (або відчули канал). Тому важливо зазначити, що місцеві рішення NR <l <NR використовуються у правилах синтезу.

$$P\{\text{рішення} = H1 \mid H1\} = P\{Q_d > \lambda | H1\}$$
$$P\{\text{рішення} = H1 \mid H0\} = P\{Q_f > \lambda | H0\},$$
де (1.8)
$$Q_f = \sum_{i=k,j}^{NR} \binom{NR}{l} P_{f,j}^{l} \left(1 - P_{f,j}^{NR-l}\right)$$
$$Q_d = \sum_{i=k,j}^{NR} \binom{NR}{l} P_{d,j}^{l} \left(1 - P_{d,j}^{NR-l}\right)$$

де Q_f та Q_d - сукупні результати прийняття зондування для хибного декларування присутності та фактичної присутності ПУ в каналі ch на ФК. λ - поріг статистики прийняття рішення (або Q_f, або Q_d), нижче якого гіпотези недійсні.

Наприклад, у [20], розглядається поріг для $\lambda > 0{,}65$. H1 і H0 позначають гіпотези відсутності або присутності первинного користувача в певному діапазоні частот, а $P_{f,j}$, j та $P_{d,j}$ - показники точності, пов'язані з індивідуальним рішенням, для j-го ВК. У цій главі передбачається, що виявлення енергії використовується для виявлення присутності ПК [21]. При виявленні енергії, якщо енергія виявленого сигналу вищепоріг, тоді оголошується, що ПК присутній. Точність рішень для H1 та H0 визначається $P_{d,j}$ та $P_{f,j}$ відповідно. ЦС оголошує спектр доступні, якщо всі рішення спільних користувачів вказують як доступні. При використанні правила OR, якщо є принаймні один користувач, який вказує канал вакантним, ЦС оголошує його доступним. Правило більшості вимагає щонайменше половини кооперативних користувачів повідомляти канал про вакантність. Ці прості правила синтезу можна узагальнити на l з правила NR (для Q_f та Q_d див. Рівняння 1.8). Коли l приймається за 1 і NR, правило l із NR стає правилом OR або AND відповідно. Правило більшості можна отримати з правила l з NR за умови, коли $l \geq \frac{NR}{2}$.

1.5 Характеристика та ідентифікація даних зондування спектру Поведінка атак фальсифікації (SSDF) за допомогою БМД

У цьому розділі БМД використовується для характеристики поведінки атак фальсифікації даних зондування спектру. Три типи поведінки атак SSDF [22], які використовуються для аналізу, описані нижче:

1) завжди в атаці де зловмисний користувач завжди посилає "1", щоб вказати, що канал зайнятий ПК. Корисливий користувач може цим скористатися і витрачає ресурс спектру. Передбачається, що період зондування каналу може бути різним. Отже, відповідь співпрацюючого користувача залежить від різного періоду зондування. Завжди включенийзловмисник, надмірно жадібний з точки зору отримання доступу до каналу. Оскільки відповідь завжди 1, максимальне значення A3 дорівнює 1. Цей зловмисник не відповідає, значення A2 також може приймати максимум 1. Зловмисник завжди повідомляє про те, що ПК працює, значення A_1 протягом періоду зондування буде еквівалентно $P_{f,i}$. Отже, знаючи можливі

значення A_1^*, A_2^*, A_3^* очікувані значення ці атрибути (тобто A_1, A_2, A_3) обчислюються, як показано в таблиці 1.3.

2) завжди вимкнена атака де зловмисний користувач завжди посилає "0", щоб вказати, що канал вільний, коли насправді він зайнятий ПК. Зловмисник відповідає під час кожного зондування спектру, значення A_2 залишатиметься рівним 1. Зловмисник прагне порушити корисність ресурсу спектру помилково.

Оновлені атрибути в моменти часу t, (t - τ) позначаються як A_i та A_i^* відповідно вказуючи доступний канал. Отже, для A_3 потрібно мінімум 0. Оскільки цей зловмисник завжди вказує, що спектр є вакантним, A_1 еквівалентно $(1 - P_{f,i})$:

1) завжди помилкова атака завжди надсилати протилежні результати зондування, які спричиняють обидва спектри втрати та перешкоди для передачі. Оскільки зловмисник реагує під час кожного зондування спектру, значення A_2 залишатиметься рівним 1. Оскільки зловмисник вказує на протилежності стану каналу (тобто заповнення та доступність) доступний канал виявляється помилково і зайнятий канал помилково оголошується доступним. Отже, A_2 приймає значення $(P_{f,i} + P_{m,i})$. Оскільки приріст корисності має однакову ймовірність бути використаним чи невикористаним, A_3 приймає значення 0,5.

2) Для надійного ВК очікувана поведінка з точки зору A_1, A_2 і A_3 може бути описана наступним чином. Для A_1 надійний ВК рідше надає дані зондування фальшивого спектру. Для A_2 рівень чутливості ВК залишається максимальним. Для A_3 жадібність збільшиться, оскільки ВК отримує доступ до доступного спектру з ймовірністю доступу $P_{d,i}$.

Виходячи з вищезазначеного обговорення, три поведінки атак та очікувана поведінка надійного користувача, що характеризується за допомогою БМД, зведені в таблицю 1.3. Кожна поведінка представлена атрибутами A_1, A_2, A_3 в момент часу t. Потім, через час зондування τ, оновлені атрибути представляються як A_1^*, A_2^*, A_3^* (у момент часу $(t - \tau)$). Передбачається, що кожна поведінка атак SSDF поступово обчислюється з використанням трьох атрибутів БМД.

Таблиця 1.3 - Представлення поведінки атак SSDF на основі атрибутів БМД

Поведінка	Оновлені атрибути		
	A_1	A_2	A_3
Завжди в атаці	$\frac{A_1^* + P_{f,j}}{2}$	$\frac{A_2^* + 1}{2}$	$\frac{A_3^* + 1}{2}$
Завжди вимкнена атака	$\frac{A_1^* + (1 - P_{f,i})}{2}$	$\frac{A_2^* + 1}{2}$	A_3^*
Завжди хибна	$\frac{A_1^* + (P_{f,i} + P_{m,i})}{2}$	$\frac{A_2^* + 1}{2}$	$\frac{A_3^* + 0.5}{2}$
Довірена ВК	$\frac{A_1^* - P_{d,i}}{2}$	$\frac{A_2^* + 1}{2}$	$\frac{A_3^* + P_{a,i}}{2}$

1.6 Ефективність характеристики поведінки атак SSDF до Визначте зловмисних користувачів

Запропонований БМД порівнюється з розрахунком довіри, запропонованим у [20]. Для порівняння використовується метрика довіри, запропонована у [20] інтерпретується наступним чином.

Три поведінки атак SSDF та довірена поведінка ВК відповідають чотирьом різним контекстам, які можуть характеризуватися різними позитивними та негативними оцінками поведінки [20]. $P_{f,i}$ еквівалентно E1 у [20] та $P_{m,j}$ (або $(1 - P_{d,j})$ еквівалентно E2 у [20]. Автори заявляють два залежні від контексту фактори забуття, що відповідають поведінці атак завжди та завжди. Оскільки автори в [20] не вказує переваг контекстно-залежних факторів забуття,

передбачається, що зловмисник не змінить свою поведінку між різними типами поведінки атаки.

Також передбачається, що зловмисник не виявляє більше однієї поведінки атаки одночасно.

Атакуюча поведінка моделювалася шляхом варіювання значень атрибутів, як описано в таблиці 1.3 для задоволення зловмисної поведінки.

Три поведінки атак порівняльно аналізуються шляхом підбору статистичних розподілів (таблиця 1.4) і порівняно із встановленим розподілом до очікуваної поведінки користувача довіри (як зазначено в таблиці 1.3).

У порівнянні для аналізу використовується дивергенція Куллбека-Лейблера (KLD) різниця у розподілі ймовірностей. KLD - це статистичний показник, який показує, наскільки близький розподіл ймовірностей до розподілу кандидатів [23].

Як показано в таблиці 1.4 представлена поведінка атаки та очікувана не зловмисна поведінка.

Стандартна похибка значень наближення порівнюється в таблиці 1.4.

Стандартні значення похибки обчислюються для кожного статистичного показника (наприклад, середнє значення, дисперсія) залежно від статистичного розподілу. Кожен статистичний показник вказаний для відповідного розподілу в таблиці 1.4.

На основі цих результатів можна зробити висновок, що стандартна помилка є мінімальною, коли поведінка апроксимується розподілом Вейбулла з різними значеннями для статистичних показників.

Для порівняння із контекстно-залежним довірою, поясненим у [20], стандартне наближення похибки для бета-розподілу порівнюється.

На основі стандартних значень помилок очевидно, що бета-розподіл добре пояснює моделі атак, але не краще, ніж розподіл Вейбулла.

Таблиця 1.4 - Характеристика поведінки атак SSDF з використанням БМД - Порівняно приблизні розподіли за допомогою Стандартної Помилки (СП), що відповідає параметрам конкретного розподілу (де a_i та b_i (де i = 1, 2, 3, 4) - параметри відповідних розподілів).

Поведінка	СП приблизних розподілів			
	Бета (a_1, b_1)	Гамма (a_2, b_2)	Вейбулл (a_3, b_3)	Ненормальний (a_4, b_4)
Завжди	(0,093, 0,292)	(0,13, 0,004)	(0,005, 0,054)	(0,024, 0,015)
Завжди вимкнено	(0,086, 0,454)	(0,084, 0,004)	(0,004, 0,042)	(0,022, 0,016)
Завжди хибна	(0,168, 0,757)	(0.165, 0,0022)	(0,0033, 0,053)	(0,026, 0,0184)
Не зловмисний	(0,101, 0,536)	(0,097, 0,0033)	(0,0037, 0,04)	(0,017, 0,013)

Атакова поведінка, що характеризується атрибутами БМД, моделюється відповідно до таблиці 1.3 і результат статистично наближений до бета-розподілу. Тоді еквівалентні параметри $P_{f,i} \equiv E1$ та $P_{m,i} \equiv E2$ [20] використовується для моделювання. Результат статистично наближений до бета-розподілу. Порівняно встановлені розподіли бета-версій для кожного з двох розподілів. Міра KLD використовується для оцінки різниці між двома розподілами, які порівнюються (див. табл 1.5). У наступному експерименті варіація БМД може бути простежена та використана як евристична для виявлення зловмисної поведінки зловмисників SSDF.

Таблиця 1.5 - Порівняння поведінки атак SSDF за допомогою БМД та контекстно-залежної довіри [20]. α та β відповідають параметрам форми розподілу бета з використанням дивергенції Куллбека-Лейблера (KLD)

Поведінка атаки	Запропонована модель		[20]		KLD
	α	β	α	β	
Завжди	2,38	5.71	2	3.71	0,0643
Завжди вимкнено	1,74	7.31	2	3.71	0,4515
Завжди хибна	3.18	13.7	2	3.71	0,5487

Атакова поведінка (табл 1.3) були змодельовані таким чином, що для кожної ітерації будь-яка з вищезазначених форм поведінки вибирається випадковим чином. Подібним чином було проведено однакову кількість ітерацій для обчислення поведінки відповідно до еквівалентних параметрів $P_{f,i} \equiv E1$ та $P_{m,i} \equiv E2$ [20], що використовується для моделювання. Два набори даних, що генеруються з двох запущених моделювань, містять будь-який із трьох типів зловмисників, а також не зловмисних користувачів, яких можна ідентифікувати на основі відповідної поведінки. Метою цього експерименту було порівняння точності класифікації БМД з контекстно-залежною метрикою довіри [20]. Результати аналізувализ використанням різних методів класифікації, доступних у WEKA [24]. Ефективність двох моделей порівнювали з використанням точності класифікації, коефіцієнта помилково позитивних та істинних позитивних показників. За результатами (таблиця 1.7) очевидно, що серед особливостей та метрик, що використовуються для надійної ідентифікації ВК в присутності зловмисників SSDF, БМД дає найбільш точну ідентифікацію. За допомогою БМД отримано середню точність класифікації 94,83% для чіткої ідентифікації чотирьох

класів. Тому надійніше використовувати БМД для точної ідентифікації нешкідливих ВК.

Таблиця 1.6 - Класифікаційна точність БМД та контекстно-залежної моделі довіри [20]. NB - наївний Байєс, MP - багатошаровий перцептрон, TP - справжній позитив, FP - хибнийПозитивні, C1 - Клас постійно зловмисників, C2 - Клас нешкідливих користувачів, C3 - Клас постійно відключених зловмисників і C4 - Клас завжди зловмисників

Виконання	MATM Модель			[20]		
	J48	NB	MP	J48	NB	MP
Точність Класифікація	87,625%	100%	96,875%	77,125%	71,375%	72,75%
TP Rate (C1, C2, C3, C4)	(0,96, 0,775, 1,0,77)	(1,1,1,1)	(0,98, 0,925, 1, 0,97)	(1,1, 0,54, 0,05)	(1,1, 0,415, 0,44)	(0,995, 1, 0,415, 0,5)
FP Rate (C1, C2, C3, C4)	(0,007, 0,075, 0, 0,077)	(0,0,0,0)	(0, 0,01, 0,022, 0,01)	(0,002, 0, 0,15, 0,153)	(0,0, 0,187, 0,195)	(0,0, 0,168, 0,19)

Далі, показники справжньої точності вибору користувачів різних кооперативних користувачів моделі відбору порівнюються з методами, заснованими на довірі, описаними в [25][26], контекстно-залежна модель довіри [20] та [21] з БМД. Очевидно, що для БМД можна чітко ідентифікувати кожен з нихтри класи зловмисників SSDF з високою точністю.

Таблиця 1.7 - Класифікаційна точність БМД та контекстно-залежної моделі довіри [20], NB - наївний Байєс, MP - багатошаровий перцептрон, TP - справжній позитив, FP - хибнопозитивний.

Модель	Номери классів	Середній коефіцієнт FP (J48, NB, MP)	Середня норма TP (J48, NB, MP)
[25]	02	(0,9,0,9,0,85)	(0,14,0,2,0.13)
[26]	02	(0,82,0,78,0,8)	(0,2,0,23,0,26)
[21]	02	(0,7,0,7,0,78)	(0,32,0,3,0,3)
[20]	04	(0,64,0,7,0,73)	(0,09,0,098,0,09)
MATM модель	04	(0,86,1,0.97)	(0,077,0,0,12)

1.7 Ефект від вибору довіреної коаліції

Метою цього набору експериментів є показати ефективність БМД для обчислення надійності ВК та вибору ТС. Приклад: Розглянемо застосування TCRM короткого діапазону, таке як моніторинг навколишнього середовища, що стосується точного сільського господарства [27], критичний за часом моніторинг стану здоров'я [28], де сиг- погіршення міцності внаслідок вицвітання вважається мінімальним. Експеримент розпочинається, коли ФК вимагає від ВК інформацію про місцеве зондування. Передбачається, що чутливі можливості ВК слідують за гауссовим розподілом. Для кожного ВК його справжня здатність зондування моделюється гауссовим розподілом із середнім значенням 0,6 та дисперсією 0,2 [29]. Повідомлена здатність зондування для зловмисного ВК встановлена на високе значення 0,95. Початковий бал довіри для всіх вузлів встановлюється рівним 1, що представляє незнання. Sens-Час встановлення становить 20 мс. Сигнал шум встановлений на –2 дБ. В експерименті 10 каналів і 16 ВК. Розташування для

кожної ВК заздалегідь визначено як двовимірну декартову координату (у сітці 20 × 20), а ЦС розміщено на (10, 10). Кожен ВК надає ЦС рішення про місцеві зондування понад 500 транзакцій і випадковим чином вимагає доступу до вільних каналів для передачі даних. Серед 16 ВК, максимум 50% з них є зловмисними (тобто можуть виявляти будь-яку з трьох форм поведінки SSDF [22]). Для кожної наступної взаємодії кожен з трьох атрибутів оновлюється відповідно до таблиці 1.3. Місцеве відношення сигнал / шум для виявлення енергії для кожного ВК береться з даних, опублікованих у [82].

Передбачається, що при кожній взаємодії з ФК ВК надаватиме наступну інформацію, Ерезидуальну, Xj та підтвердження, надіслані кожною ВК для відстеження Дрсп, j. На підставі цієї інформації, наданої кожною ВК, передбачається, що ЦС веде облік Xj, Xtotal, Drsp, j для кожної j-ї ВК та запис Respj для кожної ВК. Коли ВК надсилають запити на доступ до вакантного каналу та, виходячи з того, надаються та використовуються ці запити, відповідна інформація aj та rj для кожної ВК також зберігається у ФК.

Потім на основі записаних даних обчислюються три атрибути довіри (A1, A2, A3) для кожного з ВК. Коли кількість зловмисних користувачів збільшується, співвідношення між не зловмисними (зловмисними) та загальним числом користувачів для розрахунку довіри на основі БМД показує зменшення (збільшення).

Коли порогове значення для оголошення довіреного користувача змінюється, розмір ТС змінюється. Результати показані на рисунку 1.1.

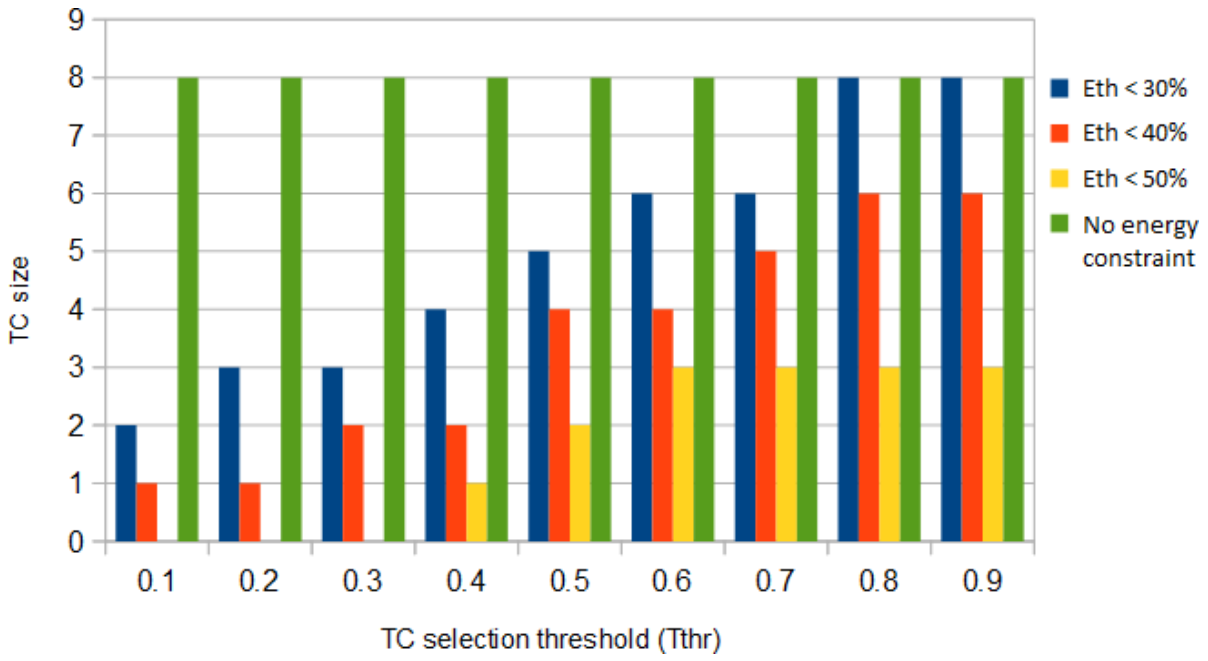


Рисунок 1.1 - Вибір ТС на основі Tthr та Eth

Як згадувалося раніше, у цій главі розглядаються правила злиття, які не ґрунтуються на консенсусі. Тому схема злиття рішень на основі довіри, описана в [29] не включається в це порівняння, оскільки пропонується для злиття рішень на основі консенсусу модель. Порівняльно аналізується показник точності прийняття рішень кооперативного зондування спектру (з точки зору Qd та Qf) для вибору ТС на основі БМД для різних правил синтезу. Порівнюється ефективність злиття рішень, коли є вибір ТС проти випадкового вибору спільного користувача (N = 8). Експеримент проводився, припускаючи виявлення енергії та апроксимацію злиття рішень за допомогою гауссової Q-функції (GQ) [30].

Як свідчать результати, ефективність покращується, коли відбувається злиття рішень на основі ТС (рис 1.2 і 1.3).

Значне покращення продуктивності показано для правила I, оскільки остаточне рішення лише 1, коли дані зондування всі 1.

Коли є ТК, продуктивність покращується. Однак розмір ТК не має суттєвого впливу на точність рішення.

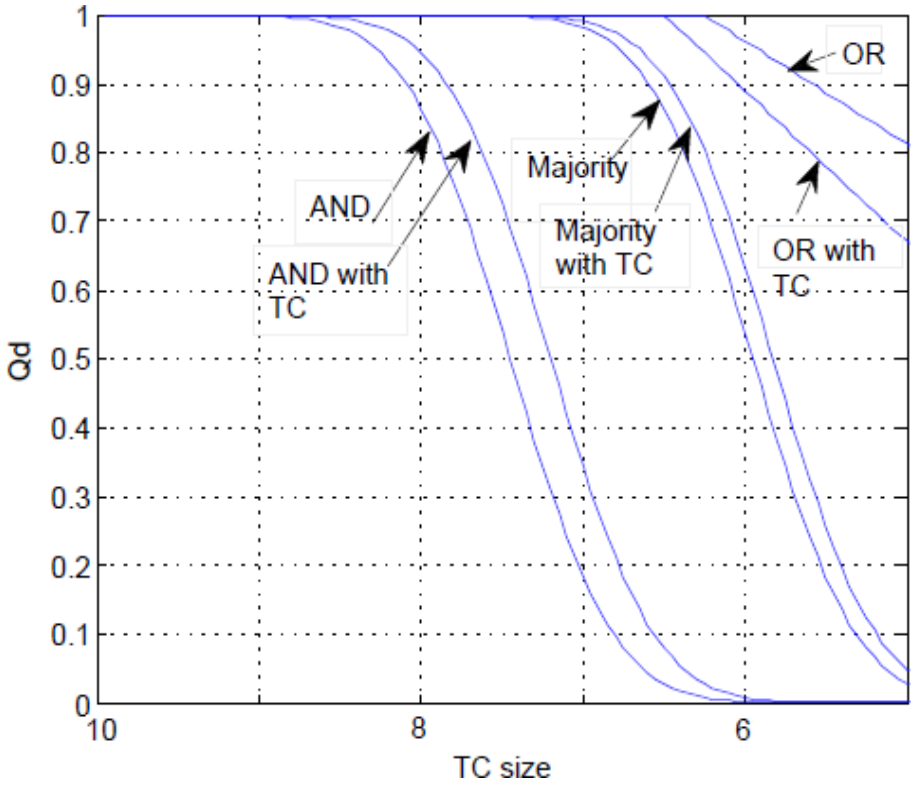


Рисунок 1.2 - Варіація Qd для різних правил злиття з вибором ТС та випадковим вибором користувача

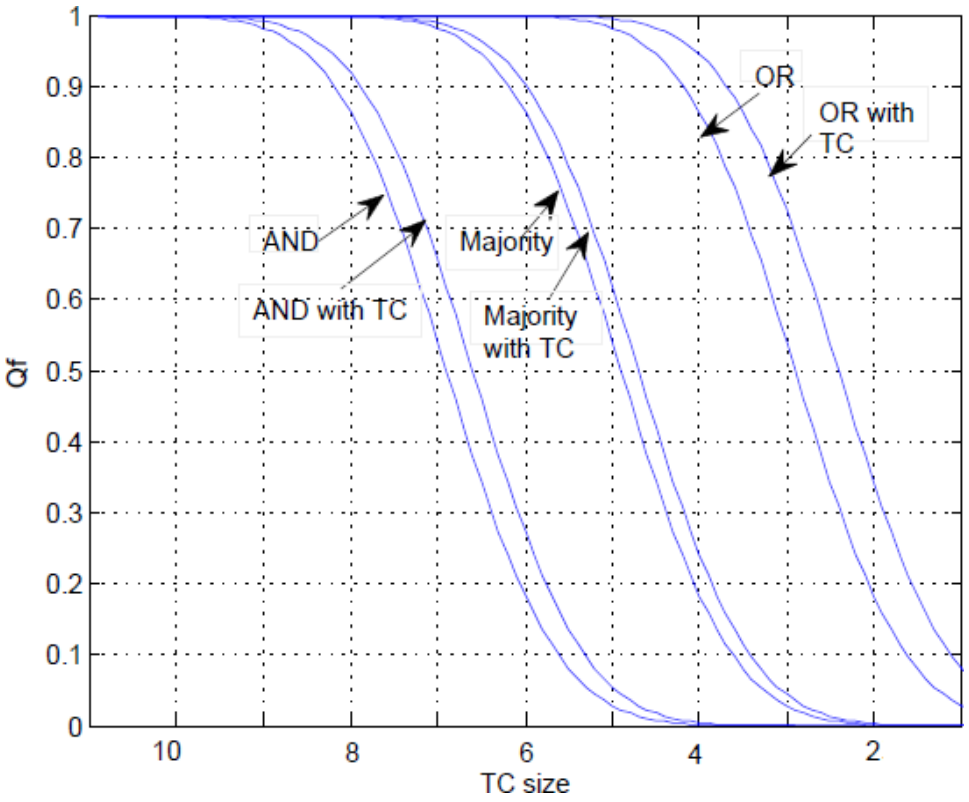


Рисунок 1.3 - Варіація Qf для різних правил злиття з вибором ТС та випадковим вибором користувача.

1.8 Аналіз затримки

У запропонованій кооперативній схемі зондування спектру на основі ТС затримка передачі вторинного користувача виникає у чотирьох випадках: зондування спектру, звіт про результати зондування, помилкова тривога і правильне виявлення ПУ. Затримка, спричинена зондуванням спектру та звітуванням, неминуча, оскільки кооперативні ВК повинні відчути спектр та надіслати результати локального зондування до ФК для прийняття остаточного рішення щодо статусу ПУ. Для обчислення затримок у двох останніх випадках формулювання, використано у [30] (Рівняння 1 і 2 у [30]) використовується там, де замість кількох інтервалів розглядається лише один часовий інтервал зондування. Для одного часового інтервалу зондування тривалості τ Pf, j (λ, τ) та Pd, j (λ, τ) обчислюються наступним чином. У рівняннях3.8 і 3.11 включені пов'язані затримки зондування. Це модифіковані версії рівнянь 1 і 2 у [30].

Для тривалості кадру T = 200 мс попередня ймовірність відсутності ПК приймається як p (h0) = 0,7, що означає p (h1) = 0,3, NR = 8. Канал із смугою пропускання 1000 Гц із використанням двійкової фази модуляція клавіш зсуву та шум рівної пропускної здатності представлений з використанням змінної Гауса з нульовим середнім значенням та дисперсією змінної, λ = 0,8, часом зондування τ = 40 мс та передбаченим tr = 0,5 ∗ τ для цілей оцінки. γ змінюється від 2 дБ до 8 дБ. Варіація середньої затримки з відношенням сигнал / шум показана на рисунку 3.4.

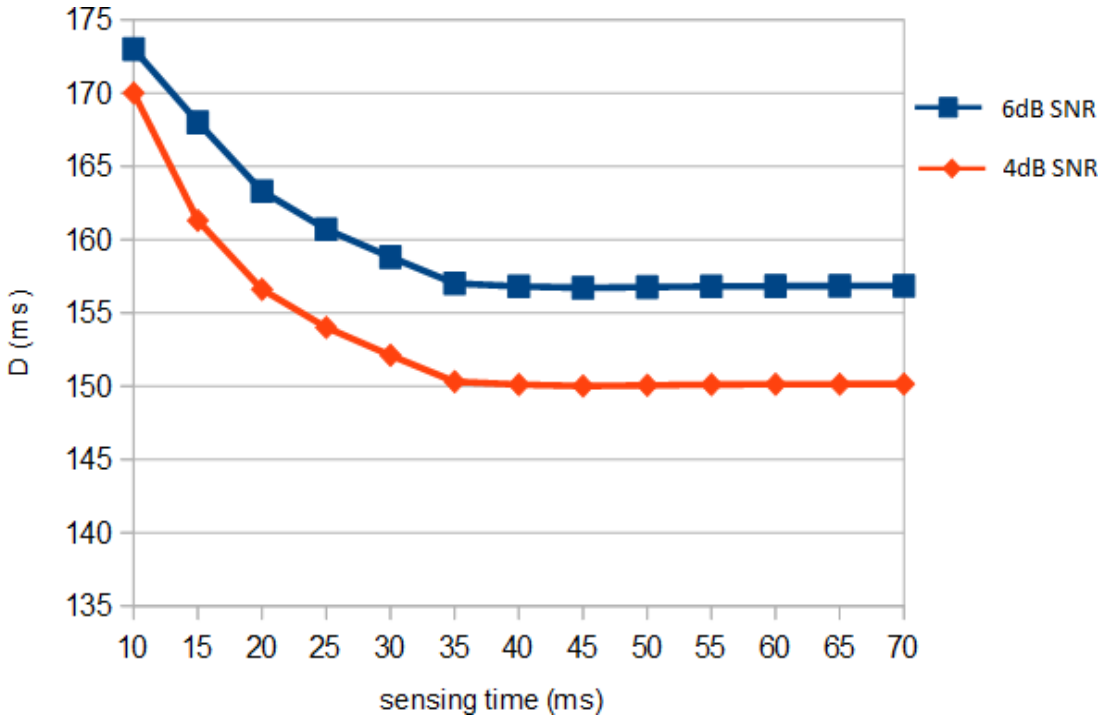


Рисунок 1.4 - Змінення затримки з часом зондування спектру для фіксованого NR = 8 та різних значень γ

1.9 Висновки

Основними внесками цієї глави є нова багатоатрибутна структура атрибутів довіри, яка, очевидно, виявляється корисною для додатків TCRM для і) вибору користувачем для спільного зондування спектру та іі) для ідентифікації зловмисників SSDF чітко на основі поведінки . Значимість цих внесків підвищує загальну надійність використання когнітивних радіомереж для затримки передачі чутливих даних у TCRMS.

2 ПОВТОРНА ПЕРЕДАЧА ДАНИХ, ЧУТЛИВИХ ДО ЗАТРИМОК

2.1 Огляд та припущення

Здача спектра керівництво виділяє вакантні канали для повторного вступу ВК для продовження передачі даних. Для встановлення доступу до вільного каналу передбачається, що загальний канал управління має достатнє покриття для всіх ВК [31]. З метою максимізаціїпередбачається, що кожна ВК може повторити спробу більше одного разу, щоб отримати доступ до спектра. Також передбачається, що кількість спроб відновити передачу повинна бути обмежена заздалегідь визначеною максимально допустимою затримкою. Крім того, робляться такі припущення.застосування загальної шини:

1) у будь-який час лише один користувач може передавати свої дані по каналу;

2) для підвищення точності виявлення доступності спектра використовується спільне зондування;

3) централізована організація спільного використання спектра приймає рішення про розподіл спектра;

4) ВК, що знову вступають, набувають вищого пріоритету, ніж ВК, що прибули на певний канал;

5) ВК не отримують доступу до спектра через менший пріоритет, ніж ПК, і ПК не існує;

6) покриття загального каналу управління досить велике для всіх ВК;

7) для конкретного каналу рівні перешкод мінімальні, а вплив джерел перешкод мінімальний.

Також вважається, що кожна ВК (наприклад, скажімо, і-та ВК) отримує дані відповідно до процесу прибуття Arri (t). Передбачається, що кожному і-му ВК потрібно передавати дані за кілька часових інтервалів. Це еквівалентно сценарію передачі великого обсягу даних. Нехай Bi (t) є відставанням у локальному буфері і-го ВК, що очікує на передачу. Коли kch кількість каналів призначено для передачі, і-й ВК передає кінцевий обсяг даних. Ємність буфера оновлюється як,

2.2 Вплив умов затухання каналу

Ємність каналу може змінюватися залежно від вицвітання та типу каналу. Відповідно до [32], для каналу, що змінюється в часі, ємність обчислюється з урахуванням кінцевого набору значень відношення сигнал / шум або SNR (γ) та пропускної здатності прийнятого сигналу (BW). Ємність затухаючого каналу визначена в [33] наступним чином коли $C\gamma = BW.\log(1 + \gamma)$ для інваріантного до часу аддитивного каналу білого гауссового шуму (AWGN). Ступінь вицвітання вказується параметром Накагамі m. Коли m = 1, сценарій такий, що канал відчуває затухання Релея. Коли $m = \infty$, канал переживає канал AWGN без затухання. Коли m переходить від 1 до 2, вираженість згасання зменшується [32]. Зв'язок між γ а m така, що для скінченної долини j така, що, $j = 1, 2, \cdots, mM \in Z, \gamma j = j + \gamma 0$, де γ0 - граничне значення SNR для підтримки оптимального рівня потужності [33]. Коли рівень затухання змінюється залежно від каналу, доступна ємність каналувідповідно змінюється. Результати наведені в Розділі 3.

Коли канал відчуває затухання, очікується зменшення потужності. Тоді час передачі збільшиться. Фактичний час передачі може збільшитися, спричиняючи більшу затримку. Однак це додаткова затримка, яка не залежить від затримки передачі спектра через багаторазові переривання.

2.3 Управління передачею спектру за допомогою декількох повторних спроб процесу підрахунку поновлення

Процес оновлення - це узагальнений процес підрахунку з незалежними однаковими часами прибуття [34]. Процес підрахунку поновлення з кінцевим очікуванням часу прибуття задовольняє закон великих чисел. Припустимо, існує кінцева кількість шансів на передачу через певний діапазон спектру протягом певного періоду. Тому доцільно використовувати процес підрахунку поновлення, щоб визначити ймовірність доступу до спектра для ВК, що входить знову.

Передбачається, що dtc - це заздалегідь визначена допустима максимальна затримка для конкретного критичного часу застосування. Для певного каналу очікується передача ВК. Передбачається, що за кількість спроб kAtt ВК може отримати доступність спектра залежно від вакантного спектру. Середня затримка обчислюється для kAtt кількості повторних спроб (див. Рівняння 4.3), де dtr, i = tsw, i + E [Twait] i з tsw, i - час перемикання, а E [Twait] i - очікуваний час очікування в черзі i-го каналу. Для обчислення достатньої кількості спроб передач підтримувати мережеві операції протягом кінцевого часу t, рівняння Уолда [35] та теорема про елементарне оновлення [36] використовуються. Припустимо кількість кінцевих спроб як mat (t), і це позначиться як функція часу. Подія повторної спроби для іншого доступного каналу може мати місце лише в тому випадку, якщо обмеження затримки не порушено. Максимально допустима затримка в окремій спробі обмежена контурою усічення dtc. Ця вимога допомагає сформулювати взаємоприбуття спроб наступним чином (Рівняння 4.4).

Далі швидкість доступу до спектра обчислюється за допомогою рівняння Вальда [35] і елементарний процес підрахунку. Відповідно до рівняння Вальда [35], а доведений результат існує як E (M) = E (X1) E (M), де M - час зупинки та E (X1) це час, коли має статися перша подія переривання. Тоді, враховуючи, що 0 <t <dtc ≤ TAtt, використовуючи рівняння Вальда [35] швидкість доступу до спектра обчислюється наступним.

Отже, Рівняння 4.6 - це мінімальна ставка для заданого значення dtc. Можна також зробити висновок, що для будь-якого іншого значення для dtc (яке задовольняє dtc ≤ Xdtc) швидкість буде більшою за мінімальну (рівняння4.6). Як тільки ВК, що повторно надходить, перевищує затримку (тобто
TAtt = dtc), зондування спектру потрібно почати знову, щоб відновити доступ до каналу як нове надходження. Після кожної повторної спроби повна затримка оновлюється, а умова i − 1 dtr, j <dtc перевірено.

Не зважаючи на деякі недоліки таких систем, UNIX-подібні ОС здатні чудово працювати в режимі багатозадачності, порівняно з ОС Windows, для використання яких необхідно безліч утиліт. Також, операційна система UNIX має високу ступінь

переносимості та надійності. Головною перевагою ОС, відносно розробки даного проекту, є підтримка симетричної роботи процесорів, що полегшить реалізацію мультипроцесорної системи.

2.4 Затримка обчислень для постійного доступу до спектру Послідовність

Як згадувалося в розділі 4.2.1, існують два типи послідовності передачі спектра: постійні та постійно змінюються. Продовжуючи рівняння 4.1, для постійного перебування отже, затримку, яку зазнав Davg за кількість перебоїв kintr, можна обчислити, використовуючи період зайнятості (Tbusy) (як еквівалентний час очікування) через поточну зайнятість каналу з високим пріоритетом та ймовірність переривання (pi) під час i-го подія переривання (Рівняння 4.7).

Застосування Формули Літтла, E [Tbusy] j для j-го каналу, можна обчислити, використовуючи співвідношення для одного сервера, що відношення між періодом зайнятості та сумою періодів простою та зайнятості дорівнює частці часу, коли сервер зайнятий . Коли існує максимальна допустима затримка для кожного повторного розгляду справи після переривання, рівняння4.7 можна переписати з точки зору d! як показано в рівнянні4.8. Передбачається, що максимальна затримка виникає при кожному повторному розгляді через переривання кінтр (тобто Davg = d!).

2.5 Аналіз надійності

У цьому розділі проводиться аналіз надійності, щоб продемонструвати найгіршу затримку для повторного вступу ВК. Передбачається, що ВК, що входять, мають вищий пріоритет, ніж ВК, що надходять, для передачі по певному каналу.

Коли спектр недоступний для повторного вступу ВК, це є недоліком, оскільки можливість передавати втрачається. Цей сценарій також можна трактувати як приниження високого пріоритету до низького пріоритету. Тому розумно припустити, що два класи ВК мають однаковий пріоритет. У такому

сценарії ВК пріоритетного класу, що повторно надходить, повинен чекати і) будь-якого ВК з високим пріоритетом, що вже знаходиться в черзі, іі) будь-якого ВК з низьким пріоритетом, що вже в черзі, і ііі) власного часу обслуговування. Подібним чином, для ВК з низьким пріоритетом є три терміни залишкового часу. Це можна узагальнити наступним чином, де Resh і Resl представляють залишковий час для класів ВК з високим та низьким пріоритетом, сервх і servl - час обслуговування ВК, yh та yl - значення заповнюваності. Оскільки час очікування $w^{-} = (R^{-}es - se^{-}rv)$, отримуються наступні результати, де Uh та Ul представляє частку часу, коли сервер зайнятий високоякісними та низькопріоритетними класами ВК. Цей результат говорить нам про те, що незалежно від контексту, ВК переживає фіксовану кількість часу очікування. Враховуючи передачу протягом часового інтервалу, значення $d! = w^{-}h$, обчислений за допомогою рівняння4.12 є найгіршим випадком очікування повторний учасник ВК, який мав намір передавати протягом цього часового інтервалу. Для будь-якого іншого сценарію час очікування менше $d! > w^{-}h$.

2.6 Експериментальне встановлення

Планування повторного вступу було змодельовано за допомогою Matlab Simulink із заздалегідь визначеними обмеженнями затримки. Модель черги та стратегії розподілу спектра (як постійно діючі, так і постійно мінливі послідовності доступу) були реалізовані за допомогою бібліотеки SimEvent. Час обслуговування є експоненціальним розподілом і прибуттями, які слідують за розподілом Пуассона. Максимальна завантаженість черги варіюється, а ефективність затримки порівнюється. Основною метою експериментів було продемонструвати доцільність запропонованої моделі та її ефективність у адаптації до різних обмежень затримки.

Методи планування є порівняно з визначенням найбільш підходящої стратегії планування для черги повторних учасників. Як описано в розділі4.2.1, Порівнюються найперші терміни, спочатку найменша розпущеність, спочатку максимальна терміновість, модифіковані спочатку найменш в’ялі методи

планування. Два показники ефективності вимірюють коефіцієнт успіху та використання [37] [38] системи використовуються для порівняння ефективності кожного методу планування.

2.7 Результати і Обговорення

Як описано в розділі 2.2, відставання залежить від нових даних (Xi (t)) та доступної ємності каналу (див. Рівняння 2.1). ефект затухання на доступну пропускну здатність каналу та відставання показано в наступних результатах (див. рисунок 2.1). Цей аналіз розглянемо варіацію вицвітання, як описано в [32], коли m = 1 - m = 2. На підставі результатів видно, що при зменшенні інтенсивності затухання доступна пропускна здатність каналу збільшується і призводить до зменшення загального відставання.

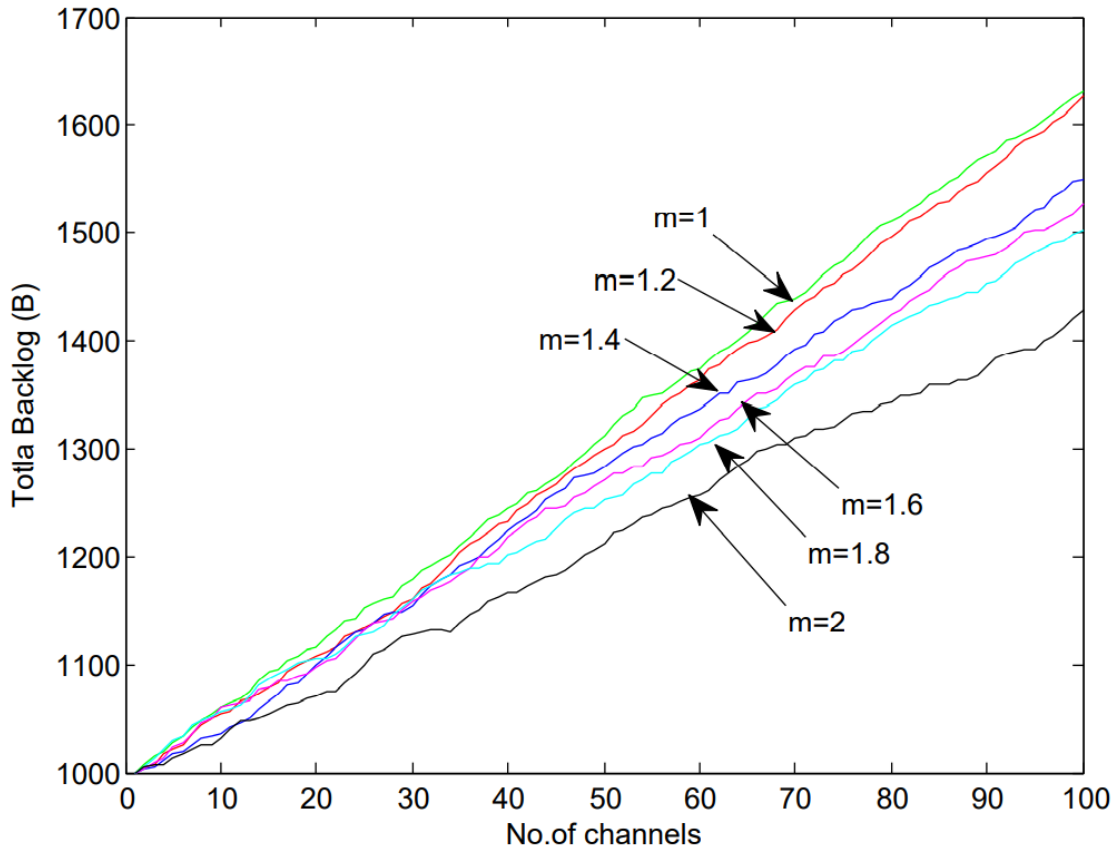


Рисунок 2.1 - Вплив затухання на доступну ємність каналу (C) та відставання (B) для фіксованих нових блоків даних про прибуття

Як показано на рисунку 2.2, описані результати повторного вступу ВК та їх спроб для одного вакантного каналу з точки зору обмежень затримки. У цьому конкретному екземплярі моделювання є три повторні спроби, і відповідний шаблон взаємодії відображається в 2.2. Далі, варіація кількості повторних учасників, коли є кілька вакантних каналів і the відповідний прераж вайтинг час (w^{-}) є показано на рисунку 2.3.

Як показано на рисунку 2.4, варіація dtr, і порівняльно аналізується на предмет постійних змін на основі послідовності спектру управління передачею. Коли pi - велике значення, dtr, і збільшується. Коли час обслуговування займає експоненціальний розподіл, вплив pi на збільшення dtr, і зменшується порівняно. Однак варіація dtr, і зменшується на $0{,}1 \leq pi \leq 0{,}5$, коли значення dtr, і збільшуються із збільшенням кількості повторних випробувань (kAtt) до дев'яти (09).

Як показано на рисунку 2.5, коли пі збільшується, dtr, і також збільшується. Порівняно з фіксованим значенням Tbusy, коли воно приймає експоненціальний розподіл, загальний dtr, і в останньому випадку значно нижчий. Можна також зробити висновок, що коли кількість повторних судових процесів перевищує шість затримка зменшується для будь-яких $0{,}1 \leq pi \leq 0{,}9$.

Порівняння змін затримки в постійному та постійно мінливому секторі спектра квантів для управління передачею, можна зробити наступні умовиводи. По-перше, можна зробити висновок, що pi є значущим фактором, який сприяє високим значенням dtr, i. По-друге, для постійно мінливих послідовностей спектру затримка відносно зменшується для експоненціального розподілу часу обслуговування. По-третє, коли кількість повторних спроб збільшується при різних порогах, політика планування на основі EDF стає найбільш ефективною, оскільки затримка зменшується до нуля.

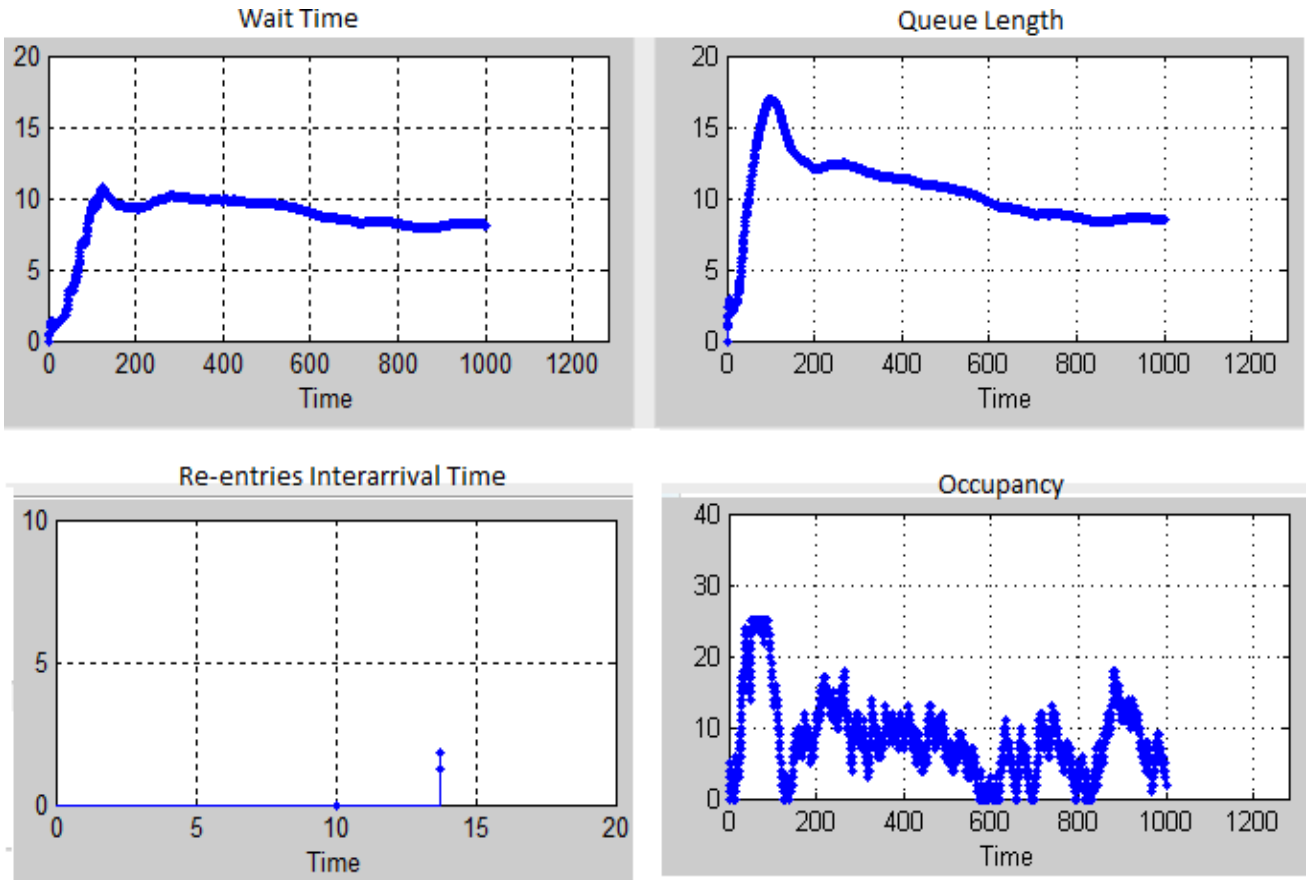


Рисунок 2.2 - Сценарій симуляційного експерименту - результати перепланування високопріоритетних ВК в моделі черги зворотного зв'язку на основі пріоритетів з одним каналом. У цьому конкретному сценарії ймовірність блокування дорівнює 0. Максимальна заповненість черги – 25

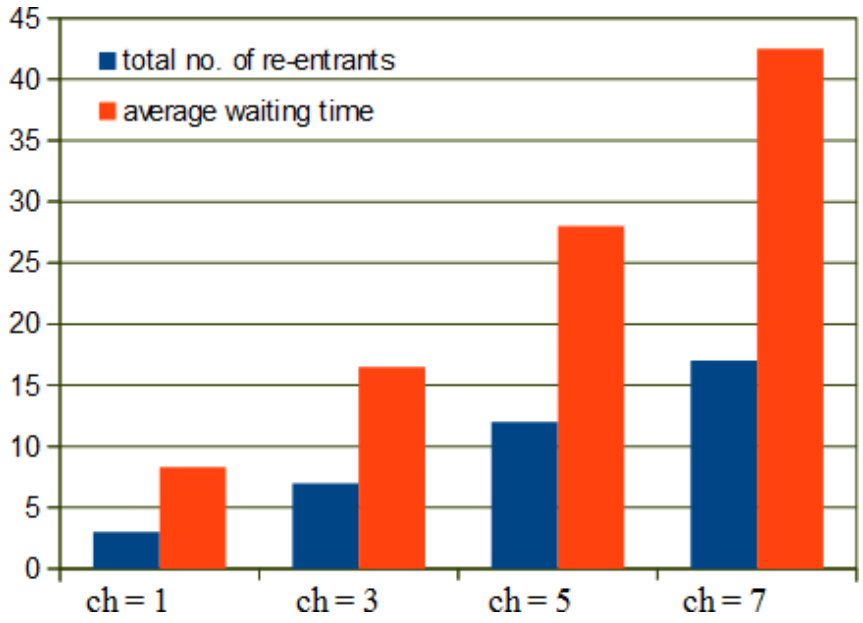


Рисунок 2.3 - Варіація загальної кількості повторних учасників та середнього часу очікування ($\bar{w}$) для різної кількості вакантних каналів

Далі порівнюють середню затримку запропонованого методу повторного випробування, чутливого до затримки.

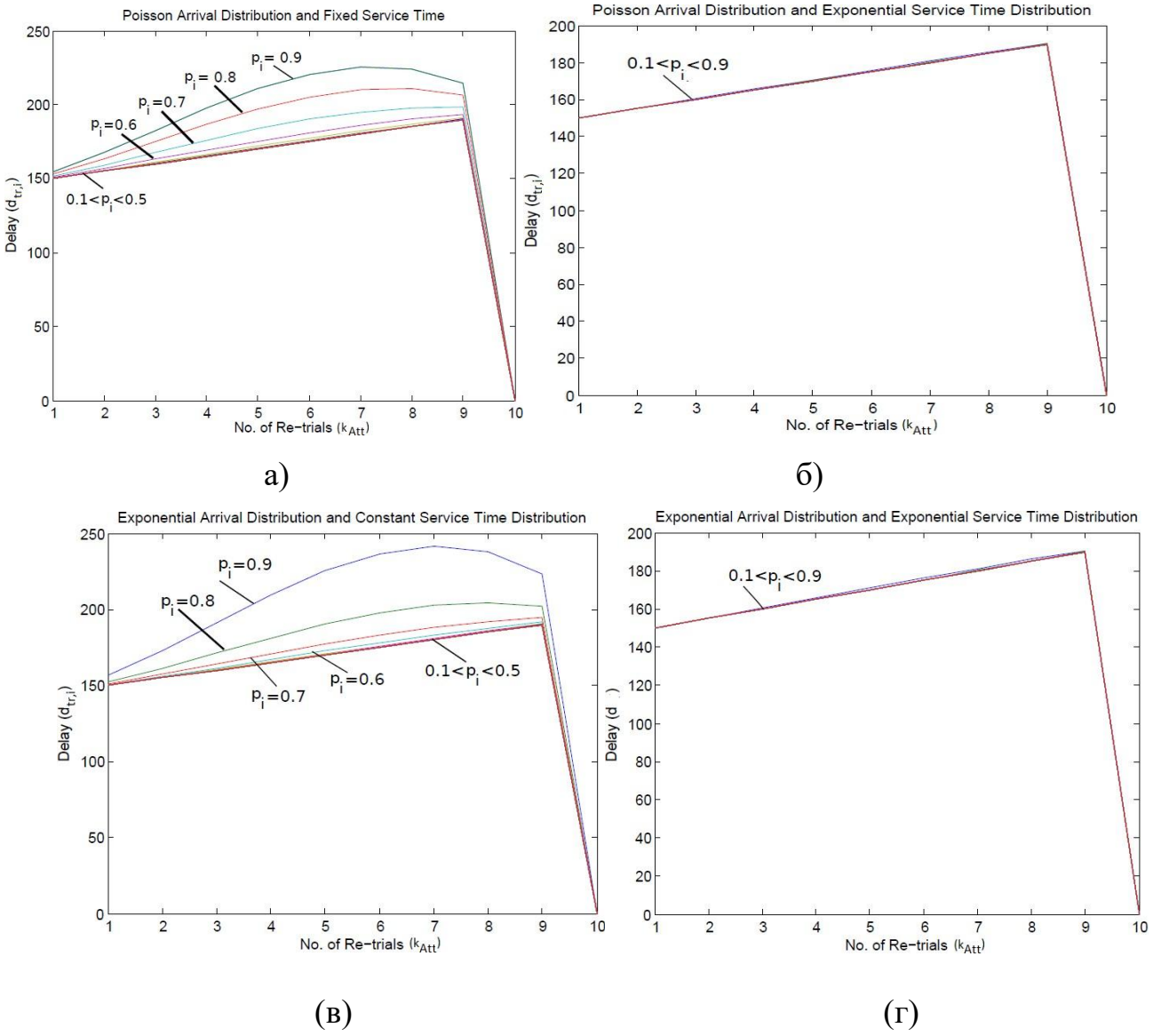


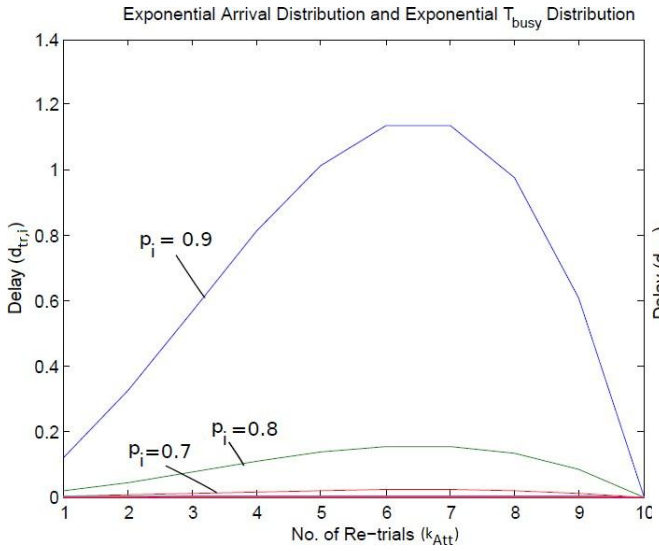
Рисунок 2.4 - Аналіз затримки (dtr, i) постійно змінюваної послідовності доступу до спектру з кількістю повторних випробувань (kAtt). Наведені результати для різних розподілів часу прибуття та часу обслуговування для різних ймовірностей переривання (pi)

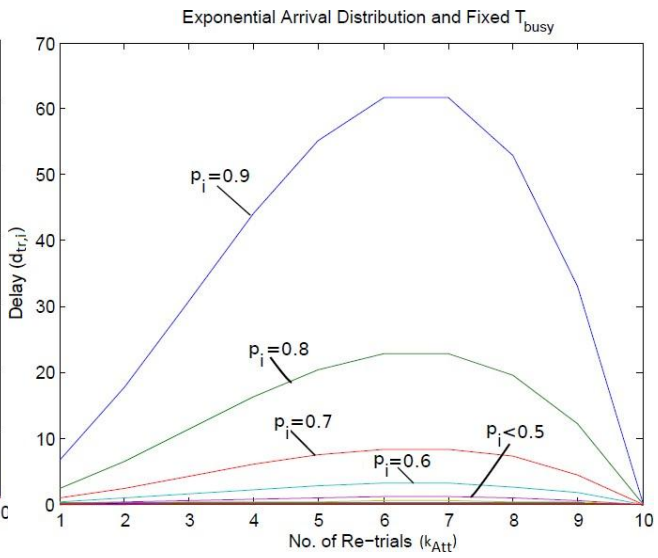
Як зазначалося раніше, [58] розглянемо максимум 5 переривань. В експерименті використовується одна черга переважного пріоритету сервера з експоненціальним приходом та часом обслуговування. Мешканці мають присвоєні мітки пріоритетів. Повторно в'їзні ВК мають вищий пріоритет, ніж нові

надходження ВК. ПУ має найвищий пріоритет. Прибуття ПУ є випадковим. Максимально допустима затримка ВК встановлена як d! = 30 і час перемикання каналу вважається дуже малим порівняно із затримкою. Робота [58] та запропонований спосіб порівнюються на основі очікуваної затримки для кожного користувача у розкладі з пріоритетними користувачами.

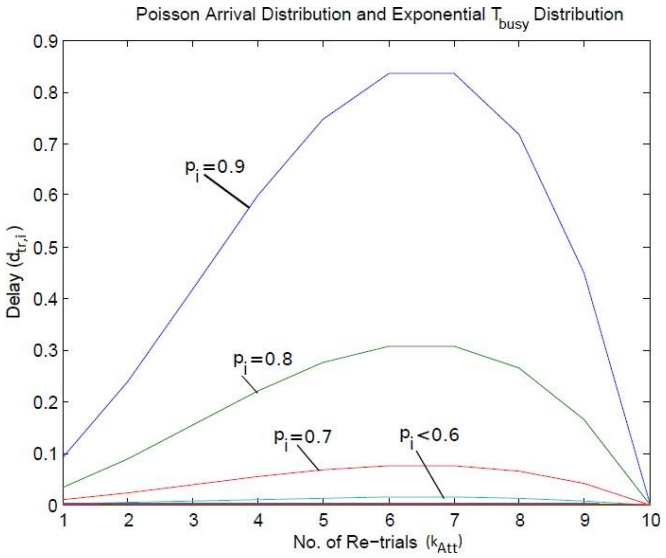
Таблиця 2.2 - Порівняння варіації середньої затримки, коли (i) кількість нових надходжень ВК зафіксовано (розглядається 06) та (ii) кількість нових заїздів ВК змінюється (кожен рядок відповідає до 6, 8, 10 нових надходжень ВК)

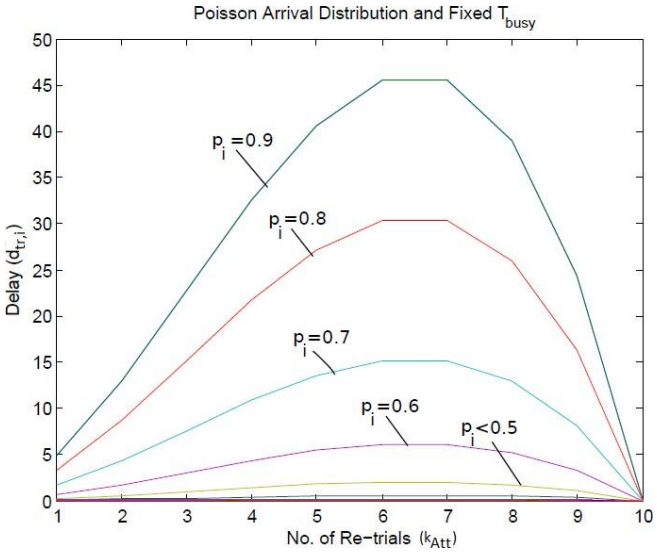
Повторні учасники	Середня затримка (и) із використанням запропонованого методу			
	ForRe-учасник (i)	ForNew ВК (i)	ForRe-учасник (ii)	ForNew ВК (ii)
3	16.8	58.2	16.8	58.2
5	28.2	70.1	28.2	72,8
7	42,5	84,5	42,5	104.2





(а) (б)





(в) (г)

Рисунок 2.5 - Аналіз затримки (dtr, i) аналізу послідовності доступу, що завжди залишається. Показано результати для різних розподілів прибуття та (Tbusy) для різних ймовірностей переривання (pi). не планується на основі затримки, а з фіксованим вищим пріоритетом, ніж нові ВК в черзі. У запропонованому методі всі ПС плануються на основі заздалегідь визначеного критерію (наприклад, термін, терміновість)

На основі результатів, наведених у табл. 2.2, коли пропонується метод, обмежений затримкою використовується затримка, що зазнала за рахунок повторних вступників збільшується, коли або кількість в’їжджаючих зростає, або коли черга стає більшою з приходом нових ВК.

Далі продуктивність різних Методи планування емпірично оцінюються, щоб визначити, які можуть запропонувати найменшу можливу затримку як для повторного вступу, так і для нещодавно прибулого ВК.

У цьому експерименті максимальна затримка та максимальний час виконання дорівнюють 100. Час виконання експоненційно розподіляється з очікуваним значенням 15. Тривалість часу завдання призначається з діапазону (максимальний час виконання, максимальна затримка) з рівномірною ймовірністю розподіл. Терміни призначаються залежно від тривалості виконання цього завдання.

Середні значення показників ефективності обчислюються після 300 повторних експериментальних випадків.

Рисунок 2.6 показує ефективність планування методи. На основі результатів, MUF є більш надійним для планування повторного вступу, оскільки коефіцієнт успішності вищий, ніж інші три методи.

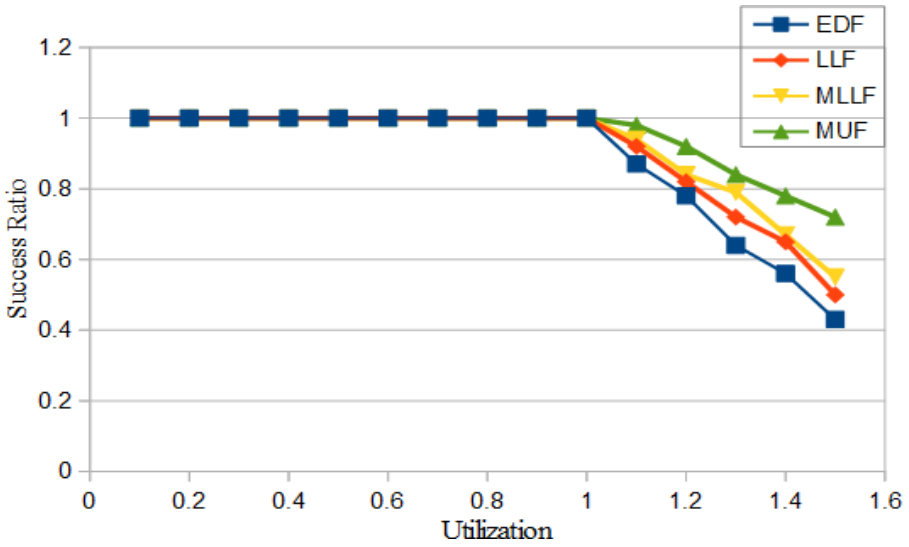


Рисунок 2.6 - Порівняння різних методів планування повторного вступу (найперший термін - перший (EDF) [40], спочатку найменша в'ялість (LLF) [41] [42], максимальна терміновість спочатку (MUF) [37] та модифікована спочатку найменша в'ялість (MLLF) [42]). Показники ефективності - це співвідношення успіху та використання [37] [38]

2.8 Висновки

Можлива кількість спроб у межах відомого обмеження затримки обчислюється за допомогою процесу підрахунку поновлення. Основне припущення полягає в тому, що максимально допустима затримка встановлюється вдвічі більшим за можливий час зондування активного спектру [43], що розглядається як 30-ті роки [44].

Максимальна кількість повторних спроб обмежена дев'ятьма (09) при максимально допустимому затримка встановлена на 30 секунд за умови, що час перемикання каналу дуже малий. За тієї ж максимально допустимої затримки, постійний підхід до передачі може дозволити до шести (06) повторних випробувань.

3 НАДІЙНИЙ ВИБІР ПОСТАЧАЛЬНИКА ІДЕНТИФІКАЦІЙНИХ ДАНИХ НА ОСНОВІ ДОВІРИ

3.1 Metric01 - Довіра на основі вразливості до загрози

Для постачальника ідентифікаційних даних більший вплив на уразливі місця є ознакою більшої схильне ненадійне розкриття вірчих грамот. Ставлення до ризику може якісно описати ставлення постачальника ідентифікаційних даних до протистояння потенційним уразливостям, незважаючи на це встановлені засоби безпеки (наприклад, брандмауери, системи виявлення вторгнень, мережа аномальний фільтри трафіку). Різне ставлення до ризику корисно для якісного порівняння потенційних вразливих місць [45]. Існує три різні відносини до ризику: (i) несхильний до ризику, (ii) схильний до ризику та (iii) нейтральний до ризику. Неприязнь до ризику - це неприязнь до ризику. Любити ризик - це більша ймовірність ризикувати. Ставлення до ризику - це лише описова маркування форми характерної функції [46], що описує поведінку фактора ризику в конкретній ситуації. У цій главі відносини до ризику використовуються для опису кожного з факторів моделювання атаки [47] [48]. Загалом,атака моделюється з використанням чотирьох факторів:

1) ризик здійснити атаку (наприклад, розкриття особи зловмисника);
2) вартість виконання атаки (наприклад, витрачений час);
3) ранг супротивника визначається виходячи з навичок, використовуваних інструментів та попередніх випадків атак та
4) стимули, отримані противником, розпочавши атаку.

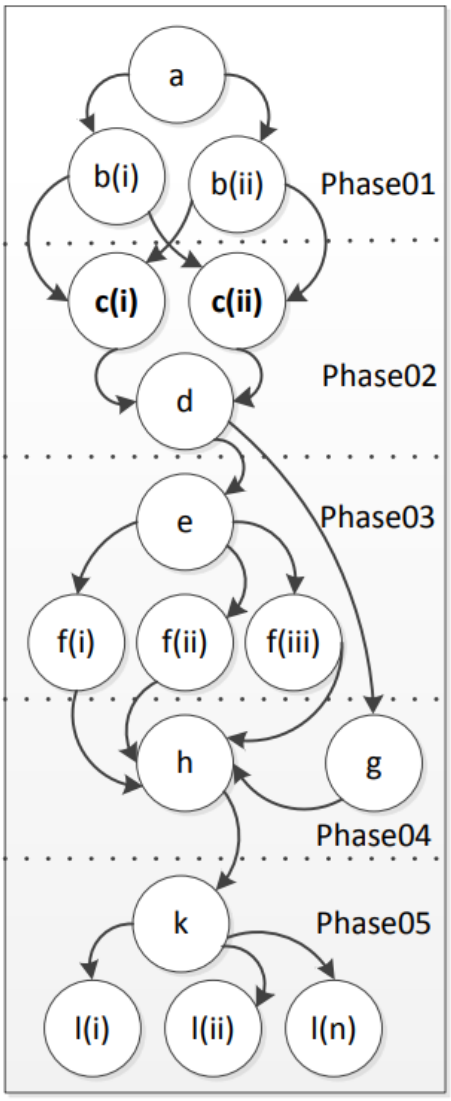
Звання суперника та потенційні стимули відповідають позиціям, що люблять ризик. Коли ранг нападника вищий, це збільшує ймовірність успішної атаки. Вартість і ризик початку атаки відповідає позиції, яка не допускає ризику. Наприклад, зловмисники частіше використовують менш складні інструменти, такі як Extensible Markup Language - Denial of Service (X-DoS) через відсутність реального захисту. З іншого боку, ризикуюче ставлення супротивника описує вартість або інвестиції для успіху певних атак. Однак вкладений час суттєво

збільшує шанси на зловлення та ідентифікацію супротивника, що вказує на те, що фактор ризику моделюється як поведінка, несхильна до ризику. Отримані заохочення можна визначити як задоволення (наприклад,

Для постачальника ідентифікаційних даних значення Metric01 обчислюється як середнє відношення до ризику (RAj), що відповідає факторам моделювання атак, що сприяють (j = 1, 2, 3, 4, 5) для кількості атак Natt (рівняння 6.8). Більше значення для Metric01 вказує на те, що надійність постачальника ідентифікаційних даних менша, тоді як нижча величина відповідає вищій надійності рівень.

Приклад. Розглянемо опубліковані дані атак DDoS (розподілене відмова в обслуговуванні) [62]. Прогрес DDoS-атаки являє собою ряд кроків із конкретними шкідливими цілями (або результатами). На кожному кроці зловмисник прагне досягти часткового результату. Якщо всі кроки виконані без помилок, атака оголошується успішною, що означає, що заплановані цілі (або стимули) атаки були досягнуті. На основі набору даних 2000-1.0 даних DDOS-атаки [в кіберсистемах та MIT 2000 рік] показує, що перша фаза нападу сприяє здебільшого успіху чотирьох наступних фаз (рис 3.1). Очевидно також, що просто наявність ресурсів цього не робитьзапевнити атаку в успіху. Наполегливість і можливості зловмисника також визначають успіх нападу. Другий набір даних DDoS-атаки 2000–2,0 показує, що на п’ятій фазі атаки, якщо зловмисник не триває протягом декількох годин, атака може не мати успіху. Отже, при оцінці вразливості до загрози безпеки слід враховувати ранг супротивника (змодельований мотивом атаки), вартість (моделюється як споживання ресурсів), вигоди для зловмисника та потенційні втрати для жертви.

Новиною розрахунку довіри за допомогою Metric01 є застосування ставлення до ризику для кількісної оцінки можливих сценаріїв втрати надійності постачальників ідентифікаційних даних, що відповідають до відомого набору атак. Кожен сценарій описаний з використанням вищезазначених факторів моделювання атак. Розроблена система нечітких висновків для визначення внеску кожного з цих чотирьох факторів для обчислення ступеня вразливості загрози безпеці постачальника ідентифікаційних даних.



a – HINFO Query
b(i) – sadmind attack will work
b(ii) – correct stack pointer
c(i) – append user to a password file
c(ii) – append user to a shadow password file
d – sadmind attack breaks into Eyrie DNS server
e – ftp to mill
f(i) – break into Solaris host
f(ii) – break into mstream server
f(iii) – break into mstream master software
g – telnet to mill
h – launches script and break into Solaris hosts according to HINFO records
k – manually launch DDoS attack
l – attack each victim by flooding packets

Phase	Cost	Benefits	Loss	Rank
01	**Low**	**Very High**	**High**	High
02	Moderate	High	High	High
03	Moderate	Very High	High	High
04	High	High	High	High
05	***Very High***	High	***Low***	High

Рисунок 3.1 - Набір даних 1.0.2000 - П'ятифазний сценарій DDoS-атаки, де зловмисник перевіряє мережу, проникає до хоста, використовуючи вразливість Somaris sadmind, встановлює троянське програмне забезпечення DDoS mstream і запускає DDoS-атаку на сервері поза сайтом від скомпрометованого хоста. Показує графік залежності та умовиводи щодо чотирьох ознак: рейтинг, вартість, вигоди та збитки

3.2 Metric02 - Довіра на основі стійкості до стійкості

Незважаючи на те, що постачальник ідентифікаційних даних є вразливим, можуть бути вже встановлені заходи безпеки (наприклад, брандмауер, фільтри трафіку, системи виявлення вторгнень) для виявлення або пом'якшення певні типи

атак. З цієї точки зору, основні обмеження використання Metric01 включають наступне:

1) вимагати достатньої кількості даних, щоб отримати необхідну інформацію про фактори моделювання атак та пов'язані з ними типи ризиків;

2) вже реалізовані заходи щодо пом'якшення або запобігання атакам не враховуються в розрахунку довіри.

Для вирішення вищезазначених обмежень визначено другу міру довіри, яка використовує інформацію про заходи безпеки для стратегій пом'якшення для оцінки безпеки стелс постачальника ідентифікаційних даних. Для конкретного механізму забезпечення безпеки розглядаються три фактори для розробки Metric02:

1) кількість загроз, які можна запобігти;

2) кількість загроз, які можна виявити та;

3) кількість загроз, які неможливо запобігти або виявити за допомогою механізму забезпечення безпеки.

Наприклад, розгляньте брандмауер як засіб безпеки. Очікується брандмауердля запобігання, а також виявлення набору відомих загроз безпеці [49]. Однак розуміння запобіжних та виявлених загроз безпеці, заснованих на реальних операціях, може бути менше очікуваної кількості. Ця різниця може виникнути через нові типи атак або помилки конфігурації [49]. Отже, якщо рівень безпеки, приписаний брандмауеру, повинен бути обчислений, тоді можна використовувати співвідношення відомих до очікуваних запобіжних та виявлених загроз. На основі цих значень можна обчислити рівень довіри щодо стійкості безпеки через брандмауер.

Далі описано обчислення Metric02 для конкретного постачальника ідентифікаційних даних. Проблемаздатність довіри (Ptr, j) для здійснення безпечної взаємодії завдяки застосуванню функції захисту! j !. Для кожного забезпечення безпеки воно обчислюється як відношення між кількістю відомих запобіжних, виявлених недоліків безпеки (kdsv) та очікуваною кількістю вразливостей безпеки (kesv).

Практичним обмеженням точної кількісної оцінки kdsv та kesv для вже наявних заходів безпеки є відсутність достатньої інформації. Інформація про вразливості є загальнодоступною у кількох базах даних, таких як база даних про вразливості з відкритим кодом (OSVDB), Загальний список вразливостей та опромінення (CVE) та Національна база даних про вразливості NIST. У хмарних обчислювальних платформах постачальники та розробники не завжди надають вичерпні описи всіх можливих вразливих місць, які можна запобігти та виявити, а також заходи безпеки. А також з часом виявляються нові атаки та уразливості, що ускладнює надання точного прогнозу [50] [51]. Наприклад, атаки нульового дня можна розпочати, використовуючи вразливі місця, які раніше не розкривалися [52]. У Розділі 3, допорівняти запобіжний і виявляється набір атак, використовується теорія нечітких грубих множин [53]. Будь-яке значення менше 1 вказує на мінімальне забезпечення безпеки. Коли потрібно мати більше ніж одну функцію безпеки, міра безпечності може бути інтерпретована як "низька" в якісному масштабі.

3.3 Показник витрат на основі політичної залежності (PDCM)

Політичні обмеження представлені у вигляді витрат чи накладних витрат [54] [55]. Представництво на основі витрат може оцінити потенційну недовіру, спричинену постачальник ідентифікаційних даних під час процесу переговорів про довіру. З цієї точки зору, політична залежність метрика витрат (PDCM) визначається наступним чином, де Ydomaini - це кількість залежностей політики від конкретного домену, а Cdomaini - пов'язана з цим вартість, оцінена на основі рівня складності оцінки. Подібним чином кількість субдоменів та пов'язані з ними витрати позначаються як Ysub-domaini та Csub-domaini. Більше значення для PDCM вказує на вищі залежності, які знижують надійність співпраці через обмеження залежностей.

Для того, щоб розрахувати значення для специфічних доменних політичних залежностей та пов'язаних з ними витрат, використовуються порушення угоди про

рівень обслуговування та пов'язані з ними витрати [56]. Як правило, відносини між хмарним постачальником та клієнтом регулюються Угодою про рівень обслуговування (SLA). SLA встановлюється для визначення рівня послуги та супутніх витрат. Неможливість надання послуги називається порушенням SLA. Для виявлення порушень SLA необхідно мати конкретні деталі параметрів якості обслуговування та цілей рівня обслуговування (наприклад, доступність, пропускна здатність та час реагування). За даними останньої публікації [57], надайте порушення SLA та відповідні витрати. Ці опубліковані дані використовуються для розрахунку PDCM (табл6.3). Згідно з наявними даними, в даних обчислення вартості SLA немає субдоменів, що беруть участь.

3.4 Експерименти та результати. Обчислення з Metric01.

У цьому розділі використовуються загальнодоступні дані про атаки та вразливості для обчислень двох показників довіри Metric01 та Metric02. Потім описується приклад сценарію для демонстрації методу вибору постачальника ідентифікаційних даних на основі PDCM.

Для обчислення Metric01 використовуються набори даних історії нападу [в кіберсистемах та MIT 2000 рік]. Зокрема, п'ять (05) фазових наборів даних DDoS-атаки (2000-1.0 (DS01) і 2000-2.0 (DS02)) 2000 року та два набори даних атаки "mailbomb" (ідентифікатор атаки - 42.155148) і "fdformat" (атака id - 52,16243504) 1999 року (DS03 та DS04 відповідно). Наприклад, згідно з набором даних 1998 р., Вартість з точки зору часу, необхідного для запуску атаки, приймає числове значення. Ризик, вміння та стимули мають якісне значення (високий, помірний, низький). Потім значення RAj обчислюються для кожного сценарію атаки. Нечіткі змінні здатні моделювати такі мовні декларації, як низький, середній, високий тощо [59]. Нечітке число присвоюється з діапазоном можливих значень для представлення кожного мовного дескриптора. Щоб робити умовиводи за допомогою цих нечітких чисел, правила if-then конкретно визначені. У [59], а вразливість представлена за допомогою нечіткого числа. Для обчислення Metric01 факторам моделювання атаки присвоюються відповідні нечіткі числа. Функції

членства вибираються та визначаються для кожного атрибута залежно від діапазону, який він повинен представляти. Домовленість полягає у виборі простої (тобто менш обчислювально обчислювальної) функції належності для представлення атрибута [59].

За визначенням, відношення до ризику обчислюється як відношення між першою та другою похідною характерної функціональної форми, також відомої як функція корисності [60] [61] [46]. У нормалізованому масштабі, корисність відношення до ризику приймає максимальне значення 1 і мінімум 0. Як правило, Схильність до ризику описана за допомогою увігнутої корисності функції [17]. Прикладами можуть бути логарифмічна та степенна функції. Ставлення до ризику описується за допомогою опуклих функцій корисності. Приклади включають експоненціальну та негативну функції степенів. Однак, якщо недостатньо числових даних для підтримки факторів моделювання атаки для характеристики функцій корисності, тоді слід враховувати більш гнучкі методи, які можуть враховувати описові значення (наприклад, вартість атаки висока, низька або помірна).

Таблиця 3.2 - Аналіз внесків кожного модуля атаки eling Factor (майстерність зловмисника, вартість запуску атаки (з точки зору часу) та заохочення, отримані зловмисником.)

Назва атаки	Майстерність	Вартість	Стимул
pod	низький	високий	високий
portsweep	високий	високий	високий
rootkit	високий	високий	високий
satan	високий	високий	високий
smurf	високий	високий	високий
Spy	високий	високий	високий

Кінець таблиці 3.2 - Аналіз внесків кожного модуля атаки eling Factor (майстерність зловмисника, вартість запуску атаки (з точки зору часу) та заохочення, отримані зловмисником.)

Назва атаки	Майстерність	Вартість	Стимул
syslog	високий	високий	високий
teardrop	високий	помірний	високий
warez	високий	високий	високий
warezclient	помірний	низький	високий
warezmaster	високий	високий	високий
2000 наборів даних [62]			
DDoS 2.0.2	низький	високий	низький
DDoS 1.0	низький	високий	низький
1999 Набір даних атаки стелс [62]			
eject	високий	помірний	високий
sqlattack	високий	помірний	високий
loadmodule	високий	помірний	високий
ps	високий	помірний	високий
ffb	високий	низький	високий
perl	високий	низький	високий
format	високий	низький	високий

Серед чотирьох факторів моделювання нападів розкривається ступінь ідентичності зловмисників не має достатньо даних для оцінки. Тому в цьому експерименті враховуються лише три фактори моделювання атаки. Наприклад, 1998 набір даних [в кіберсистемах та MIT 2000 рік], вартість запуску атак з точки зору нормованого часу ніколи падає нижче 0,33 або більше 1. Низькі та помірні витрати диференціюються навколо 0,43. Для досягнення максимальної ефективності проведемо наступний тест, з використанням більших вхідних даних.

Між високими витратами відрізняються помірні витрати вище 0,52.

Навичка атакуючого якісно оцінюється наступним чином: 0,7 і вище як високий, 0,5 і нижче 0,7 як помірний, від 0,3 до 0,5 як низький [63]. Відповідно до [64], на підставі симуляційних експериментів, доцільно стимулювати атаку наступним чином: вище 0,3 до 1 як “Високий”, від 0,2 до 0,3 як помірний, а найнижчий - 0.

Таблиця 3.2 показує підсумок аналізу набору даних атаки. Результатом є відношення до ризику (RAj).

Як показано на рисунку 3.3, відносини з низьким та помірним ризиком представлені за допомогою функції psigmf, вже визначеної в панелі інструментів нечіткого висновку Matlab (форма представляє поведінку, несхильну до ризику в окремому інтервалі), тоді як велике значення RAj представлено за допомогою функції sigmf, визначеної в панелі інструментів нечіткого висновку Matlab (для опису поведінка, що любить ризик).

Відповідний нечіткий висновок з використанням трапецієподібних нечітких функцій належності показаний на рисунку 3.4.

Таблиця 3.3 - Обчислення Metric01 для прикладу сценарію п’яти (05) постачальників ідентифікаційних послуг, які вразливі до різних набори загроз.

Посвідчувач	Ydомен	C.домен	PDCM
ВПО 01	3184	97,21	3,091 × 105
ВПО 02	980	106,55	1,044 × 105
ВПО 03	1916 рік	98,75	1,892 × 105
ВПО 04	464228	98,9	459,1 × 105
ВПО 05	47878	130,31	62,4 × 105
ВПО 06	53391	101,63	54,3 × 105
ВПО 07	59599	89.06	53,1 × 105
ВПО 08	327	95,29	0,312 × 105
ВПО 09	344	94.06	0,323 × 105
ВПО 10	36436	101,64	37,033 × 105
1998 Набір даних [62]			
Назва атаки	Навичка	Вартість	Стимулювання
back	низький	високий	високий
dict	високий	низький	високий
eject	низький	високий	високий
ffb	високий	високий	високий
format	низький	помірний	високий

Кінець таблиці 3.3 - Обчислення Metric01 для прикладу сценарію п’яти (05) постачальників ідентифікаційних послуг, які вразливі до різних набори загроз.

Назва атаки	Майстерність	Вартість	Стимул
ftp-write	помірний	низький	високий
guest	високий	високий	високий
imap	помірний	низький	високий
ipsweep	низький	високий	високий
land	високий	високий	високий
loadmodule	високий	високий	високий
multihop	високий	помірний	високий
neptune	високий	високий	високий
nmap	низький	помірний	високий
perlmagic	високий	високий	високий
phf	низький	високий	високий

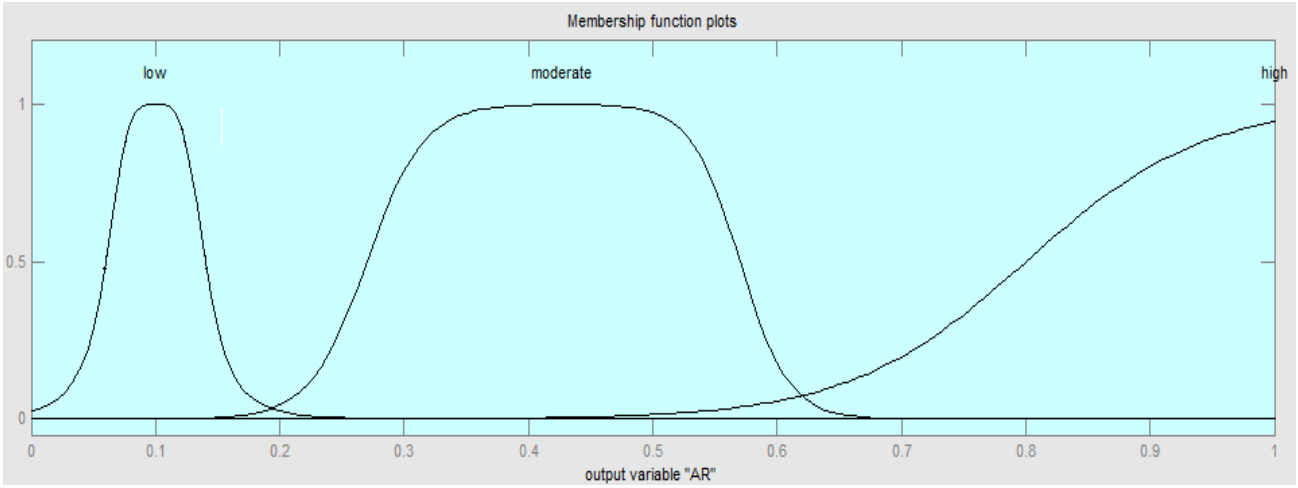


Рисунок 3.3: Функції членства для представлення RA для кожної метрики моделювання атак

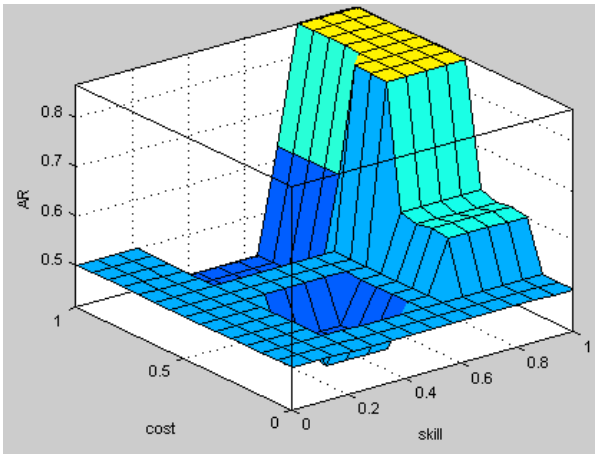


Рисунок 3.4 - Вихідні дані RA для коефіцієнта кваліфікації та фактора витрат

Щоб продемонструвати, як обчислюється Metric01, розглянемо наступний приклад наріо. Припустимо, що існує п’ять постачальників ідентифікаційних даних. Припускається, що ці постачальники ідентифікаційних даних бути вразливим до набору загроз безпеці (з табл 3.3), як показано нижче. Відповідні значення RAj для кожної (j-ї) загрози обчислюються за допомогою системи нечіткого висновку. Потім, використовуючи рівняння6.8, обчислюється значення Metric01.

3.5 Metric02 Обчислення

Для обчислення Metric02, набору атак з можливим забезпеченням безпеки та виявлення та запобігання (табл. 3.5) розглядаються.

Передбачається, що вплив (або наслідки) рівні для кожної з атак, показаних у табл. 3.5.

Потім можливий набір вразливостей було вилучено із репозиторію загальних вразливостей та ризиків (CVE) [65].

Це відносно нещодавно виявлені вразливості, і в цьому аналізі використовуються можливі засоби виправлення / попередження для зменшення впливу або їх пом’якшення.

Далі ці випадкові вразливості використовуються разом із їх виправними заходами для виведення відносних значень атрибутів для обчислення Metric02 (таблиця 3.6).

Як приклад сценарію передбачається, що набір постачальників ідентифікаційних даних має комбінацію цих заходів забезпечення, як показано в таблиці 3.6.

Таблиця 3.5 - Заходи безпеки для виявлення та попередження цього набору відомих атак

A4.	Хронометраж на атака [66] [67]	4.a) Завантаження на основі кешу гарантії	4.b) Стратегії пом'якшення на основі компілятора.	(0 - 0,9)
A5.	Атака сторонніх каналів на основі кешу [68] [69]	5.a) Виміри використання кешу у вибраних повторних кешах регіонів.	Техніки засліплення, наприклад 5.b.01) стирання кешу, 5.b.02) випадкові затримка вставки цій.	(0 - 0,9)
A6.	Міра навантаження - на основі атаки [70] [71] [72]	6.a.01) Паттерни на основі подій. 6.a.02) Кеш процесоравикористання вимірювання, 6.a.03) обчислювальне навантаження на основі виявлення спільного проживання, 6.a.04) вимірювання швидкості трафіку до серверів-резидентів	6.b) Багатосторонні переговори про безпеку на основі балансування навантаження.	(0 - 0,9)
A7.	Несанкціонована модифікація даних	7.a. Аналіз журналу брандмауера.	7.b. Потужна політика контролю доступу.	(0 - 0,9)

Виходячи з інформації, наведеної в табл 3.6, кожен постачальник ідентифікаційних даних сприйнятливий до різні вразливості незважаючи на встановлення певних функцій безпеки. Далі, використовуючи рівняння6.9, розраховуються відповідні значення Metric02 (див. табл 3.7). Тоді,загальна довіра обчислюється як сума двох відповідних значень довіри.

Таблиця 3.7: Обчислення Metric02 для прикладу сценарію п’яти (05) постачальників ідентифікаційних послуг, які вразливі до різних набори загроз та вразливостей, наведені в табл 3.6.

ВПО 01	7	12	0,583
ВПО 02	5	12	0,417
ВПО 03	9	12	0,75
ВПО 04	4	12	0,33
ВПО 05	9	12	0,75

3.6 Приклад

Розглянемо програму підтримки стихійних лих та катастроф, де для отримання необхідного аналізу та критичних рішень необхідні дані віддаленого моніторингу з кількох джерел (наприклад, супутникові зображення в реальному часі, карти) [73] [74]. Дані зберігаються у хмарних сховищах [75] [76], а користувачі аутентифікуються за допомогою цифрових ідентифікаційних даних, наданих постачальниками ідентифікаційних даних, щоб забезпечити доступ до даних. Розглянемо сценарій, коли п’ять (05) постачальників ідентифікаційних даних беруть участь у сприянні автентифікації користувачів.

Для того, щоб пояснити переговори щодо довіри та управління ідентифікацією, розгляньте керівника групи реагування на катастрофи (User01), який має отримати доступ до програми A2, щоб розподілити запити на відновлення живлення у відомому місці. Для авторизації потрібен набір з двох (02) ідентифікаційних даних атрибути: I1 та I2. Головний інженер-електрик (User02) вимагає доступу до спільної програми управління (A1) для надання ресурсів у відоме місце для того, щоб відновити живлення. Для автентифікації головного інженера (або User02) потрібні два атрибути ідентифікації I3 та I4. Для обчислення PDCM, значення в табл6.3 є використовується. Потім, для обчислення Metric02, атаки та вразливості, описані в Розділі 3 випадково присвоюються кожному постачальнику ідентифікаційних даних. Передбачається, що кожен постачальник ідентифікаційних даних схильний принаймні до однієї вразливості та однієї відомої атаки. Набори функцій захисту (див. табл. 3.3) також випадковим чином призначаються таким чином, що принаймні два набори функцій виділяються для кожного постачальника ідентифікаційних даних. Значення Metric01 обчислюється для кожного постачальника ідентифікаційних даних, як показано в таблиці 3.4. Далі, методи обчислення довіри.

Таблиця 3.6 - Оцінка відносного стелсу (Metric02) з використанням класів нечіткої еквівалентності - брандмауер (F), аналіз журналу програм (ALA), антивірус (AV), вимірювання використання кешу (CUM), фільтрація пакетів (PF), аналіз рівня пакетів (PLA) , аналіз повідомлень (MA), виявлення подій на рівні програми (ED-AL), вимірювання навантаження (LM), автоматизований механізм оновлення виправлень (АПКМ)

Посвідчувач	Технічні характеристики	Атрибути											
		A1	A2	A3	A4	A5	A6	A7	V1	V2	V3	V4	V5
ВПО 01	[F, ALA, AV,АПКМ]	0,4	0,3	0	0	0	0	0,3	0	0,7	0,7	0,7	0,7

Продовження таблиці 3.6 - Оцінка відносного стелсу (Metric02) з використанням класів нечіткої еквівалентності - брандмауер (F), аналіз журналу програм (ALA), антивірус (AV), вимірювання використання кешу (CUM), фільтрація пакетів (PF), аналіз рівня пакетів (PLA) , аналіз повідомлень (MA), виявлення подій на рівні програми (ED-AL), вимірювання навантаження (LM), автоматизований механізм оновлення виправлень (АПКМ)

ВПО 02	[F, CUM, AV, MA]	0,3	0	0,3	0	0,3	0,3	0,3	0	0	0	0	0
ВПО 03	[PLA, F, AV, АПКМ]	0,3	0,3	0	0	0,3	0,3	0,3	0	0,7	0,7	0,7	0,7
ВПО 04	[ED-AL, F, AV]	0,7	0,35	0	0	0	0,35	0,35	0	0	0	0	0
ВПО 05	[LM, F, AV, АПКМ]	0,3	0,3	0	0,3	0	0,3	0,3	0	0,7	0,7	0,7	0,7
ВПО 06	[F, CUM, PF, AV, НВАК]	0,2	0,2	0,2	0	0,4	0	0,2	0	0	0	0	0
ВПО 07	[ED-AL, CUM, F, MA]	0,5	0,3	0,3	0	0,3	0,5	0,3	0	0	0	0	0
ВПО 08	[F, PF, AV, АПКМ,НВАК]	0,2	0,2	0,2	0	0,2	0,2	0,2	0	0,7	0,7	0,7	0,7
ВПО 09	[LM,CUM, F, AV]	0,3	0	0	0,3	0,3	0,5	0,3	0	0	0	0	0

Кінець таблиці 3.6 - Оцінка відносного стелсу (Metric02) з використанням класів нечіткої еквівалентності - брандмауер (F), аналіз журналу програм (ALA), антивірус (AV), вимірювання використання кешу (CUM), фільтрація пакетів (PF), аналіз рівня пакетів (PLA) , аналіз повідомлень (MA), виявлення подій на рівні програми (ED-AL), вимірювання навантаження (LM), автоматизований механізм оновлення виправлень (АПКМ)

ВПО 10	[LM, F, AV, АПКМ, MA]	0,2	0,2	0,2	0,2	0	0,2	0,2	0	0,7	0,7	0,7	0,7

Список атрибутів V1-V5, наведених у табл. 3.6:

1) V1 - це CVE-2014-0654 Агент контекстного каталогу Cisco, відтворений обліковий запис RADIUS повідомлення Вразливість;

2) V2 є CVE-2013-6986 Невстановлена вразливість в Oracle Solaris 10 та 11.1 дозволяє місцевим користувачам впливати на доступність через вектори, пов’язані з демоном кешу служб імен (NSCD);

3) V3 - це CVE-2013-5724 Phpbb3 до 3.0.11-4 для Debian GNU / Linux використовує дозволи на запис у кеш-файлах, що дозволяє місцевим користувачам змінювати вміст файлу за допомогою стандартних операцій запису файлової системи. Ця проблема була виправлена у версії 3.0.11-4 і передбачає оновлення попередніх версій користувачів;

4) V4 - це можливий патч CVE-2014-0791. Ціле переповнення в ліцензійномучитальникуфункція в libfreerdp / core / license.cin FreeRDP через 1.0.2 дозволяє віддаленим серверам RDP викликати відмову в обслуговуванні (збій програми) або, можливо, мати неуточнені інший вплив через велике значення ScopeCount у списку обсягу в пакеті запиту на ліцензію сервера;

5) V5 - це CVE-2014-0617 Ялівець Junos 10.4S до 10.4S15, 10.4R до 10.4R16, 11.4 до 11.4R9 та 12.1R до 12.1R7 на сервісних шлюзах серії SRX дозволяє віддаленим зловмисникам викликати відмову в обслуговуванні (збій потоку) через

створений IP-пакет. Рішенням є оновлення до версії 10.4S15, 10.4R16, 11.4R9, 12.1R7, 12.1X44 або новішої, щоб усунути цю вразливість.

3.7 Порівняльна оцінка

У цьому розділі пропонуються показники (Metric01, Metric02 та PDCM) є порівняно з використанням декількох існуючих рішень з управління ідентифікацією за допомогою хмарних довіри робота [77] для федеративне управління ідентифікацією. Ця хмарна система довіри порівнює федеративну модель управління ідентифікацією, засновану на етапах до та після федерації.

Запропоновані метрики можна інтерпретувати, використовуючи хмарну систему довіри, наступним чином. Metric01 відповідає аспектам цілісності та доступності етапу до федерації. Metric01 корисний для вимірювання ступеня збереження аспектів цілісності, спроб захистити від неналежного модифікації або знищення інформації, а також для забезпечення гарантій доступності від шкідливих атак (наприклад, відмова в обслуговуванні). Metric02 відповідає наявності. Metric01 корисний для вимірювання ступеня забезпечення гарантій доступності від зловмисних вторгнень на основі історії атак та наслідків, оцінених на основі існуючих запобіжних та захисних заходів, що застосовуються конкретним постачальником послуг. PDCM відповідає аспекту оперативної сумісності. SP, який обслуговується постачальником хмарних послуг.

Далі запропоновані показники порівнюються з існуючими об'єднаними ідентифікаторами на основі хмарного рішення: SPICE [78], рішення на основі ієрархічної криптографії, описане в [79] та ICEMAN [80]. Кожне з цих рішень інтерпретується за допомогою TF [81]. Кожне існуюче рішення інтерпретується на основі TF [81] і порівняно із запропонованим управління на основі довірчих ідентифікаційних даних на основі федеративного управління ідентифікацією В SPICE [78], орієнтована на конфіденційність групові підписи з рандомізацією використовуються для встановлення автентифікації з подальшою перевіркою атрибутів, що використовуються при автентифікації. Це рішення відповідає аспектам автентифікації та підзвітності до федерації та після федерації.

У [79], федеративне управління ідентифікацією використовується з ієрархічною ідентичністю заснована криптографія, така що кожен користувач і кожен сервер матиме свою унікальну ідентифікацію, а ідентифікація призначається системою ієрархічно для ефективного розподілу ключів та взаємної автентифікації. Це рішення відповідає аспектам автентифікації та звітності перед федерацією.

ICEMAN [80] використовує існуючі хмарні API та протоколи управління об'єднаними ідентифікаторами, включаючи вказівки щодо хмарних альянсів щодо управління ідентифікацією та доступом, управління ідентифікацією як сервісу (IdMaaS) та структуру федерації ідентифікаційних даних Liberty, що підтримується ініціативою Kantara. Це рішення відповідає аспектам конфіденційності як до федерації, так і після федерації.

Підсумовуючи, результати (див. табл. 3.9) розкрити що виразність та придатність запропонованих показників у запропонованому методі вибору постачальника ідентифікаційних послуг, що базується на довірі, відповідає етапу федеративного управління ідентифікацією до федерації. Порівняння з існуючими моделями на основі хмарної моделі довіри [77] виявляє, що запропоновані показники є більш виразними у всіх трьох вимірах дофедерації фаза, тоді як інші рішення обмежуються аспектом ризику безпеки та конфіденційності.

Таблиця 3.9 - Короткий зміст аналізу виразності запропонованих трьох метрик (Matric01, Metric02 та PDCM) із використанням існуючих хмарних заснованих на довірі фреймворків (TF) [77] для хмарного управління об'єднаним ідентифікатором

Модель	Запропоновані показники	TF [77]
Запропонована модель	Метрика01	Фаза до федерації → ризики конфіденційності та приватності → Аспекти цілісності та доступності.

Продовження таблиці 3.9 - Короткий зміст аналізу виразності запропонованих трьох метрик (Matric01, Metric02 та PDCM) із використанням існуючих хмарних заснованих на довірі фреймворків (TF) [77] для хмарного управління об'єднаним ідентифікатором

Модель	Запропоновані показники	TF [77]
	Метрика02	Дофедерація фаза: → секунда-Ризики ризику та конфіденційності → Аспект доступності.
		Фаза до федерації: → Ризики знань → Прямий аспект знань.
	PDCM	Фаза до федерації: → Між-Працездатність Ризики → Операційний аспект.
PICE [78]	-	Фаза до федерації → секунда ризики конфіденційності та приватності → Аспекти автентифікації та звітності.
		Фаза після федерації → Се- ризики конфіденційності та конфіденційності → Аутентифікація та аспекти відповідальності.
Криптографія на основі ієрархічної ідентичності для взаємної автентифікації [79]	-	Фаза до федерації → секунда ризики конфіденційності та приватності → Аспекти автентифікації та звітності.

Кінець таблиці 3.9 - Короткий зміст аналізу виразності запропонованих трьох метрик (Matric01, Metric02 та PDCM) із використанням існуючих хмарних заснованих на довірі фреймворків (TF) [77] для хмарного управління об'єднаним ідентифікатором

ICEMAN [80]	-	Фаза до федерації → Ризик безпеки та конфіденційності → Аутентифікація та аспекти підзвітності.
		Фаза після федерації → Се- Курси та ризики конфіденційності → Аспект конфіденційності.

3.8 Висновки

Вклади цієї глави містять набір нових показників для оцінки надійності постачальника ідентифікаційних даних для участі в процесах автентифікації додатків TCRM. Метрики оцінювались переважно на основі загальнодоступних даних про вразливості та сценарії атак. На основі аналізів із використанням хмарної моделі довіри [77], запропоновані показники довіри та метрика витрат, що базуються на політиці, продемонстрували своє доцільне використання порівняно з іншими такими відомими існуючими хмарними рішеннями управління ідентичністю. На основі висновків цього розділу очевидно, що внески роблять хмарний доступ до даних у системах TCRMS більш надійним, коли існують ефективні методи вибору більш надійних постачальників ідентифікаційних даних.

ВИСНОВКИ

Це дослідження було розроблене для вивчення двох важливих факторів надійності: надійності та безпеки передачі даних, що сприймаються, та доступу у критично важливих для часу програмах дистанційного моніторингу. Питання дослідження стосуються обмежень існуючих методів та пропонують нові рішення, що призвели до наступних внесків:

1) багатоатрибутна довірна метрика як інструмент підтримки прийняття рішень для точного та надійного виявлення дірок спектру, уникаючи зловмисників зловмисних даних, що зондують зловмисний спектр, від участі у спільному зондуванні спектру;

2) надійна стабільна передача даних з обмеженою затримкою для повторного вступу ВК, коли є багаторазові переривання на каналах сприйнятого спектру;

3) оцінка співпраці на основі довіри для хмарного управління цифровими ідентичностями для надійної автентифікації користувачів;

Підсумовуючи, у главах 1 та 2 описуються рішення для надійної та безпечної передачі даних через ненадійні бездротові канали. У розділі 3 описані рішення в терміни надійної автентифікації користувачів із дозволами на конкретну ситуацію для надійного та безпечного доступу до даних.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. *IEEE communications magazine*. 2002. Vol. 40(8).pp.102–114.
2. I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty. Next generation/dynamic spectrum access/cognitive radio wireless networks: *A survey. Computer networks*. 2006. Vol. 50(13).pp.2127–2159.
3. I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty. A survey on spectrum man- agement in cognitive radio networks. *IEEE Communications Magazine*. 2008. Vol. 46(4).pp.40–48.
4. I. F. Akyildiz, B. F. Lo, and R. Balakrishnan. Cooperative spectrum sensing in cognitive radio networks: *A survey. Physical Communication*. 2011. Vol. 4(1).pp.40–62.
5. A. Das and M. M. Islam. Securedtrust: a dynamic trust computation model for secured communication in multiagent systems. *IEEE Transactions on Dependable and Secure Computing*. 2012. Vol. 9(2).pp.261–274.
6. X. Luo, H. Li, J. Zhang, and J. Shim. Examining multi-dimensional trust and multi- faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision support systems*. 2010. Vol. 49(2).pp.222–234.
7. W. Li, A. Joshi, and T. Finin. Coping with node misbehaviors in ad hoc networks: A multi-dimensional trust management approach. *In 11th International Conference on Mobile Data Management*, pages 85–94. IEEE, 2010.
8. T. Li and J. Du. Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing. *IET Information Security*. 2013. Vol. 7(1).pp.39–50.
9. R. L. Keeney. Multiplicative utility functions. *Operations Research*. 1974. Vol. 22(1).pp.22–34.
10. R. L. Keeney. Multiplicative utility functions. *Operations Research*. 1974. Vol. 22(1).pp.22–34.

11. I. F. Akyildiz, B. F. Lo, and R. Balakrishnan. Cooperative spectrum sensing in cognitive radio networks: *A survey. Physical Communication*. 2011. Vol. 4(1).pp.40–62.

12. I. F. Akyildiz, B. F. Lo, and R. Balakrishnan. Cooperative spectrum sensing in cognitive radio networks: *A survey. Physical Communication*. 2011. Vol. 4(1).pp.40–62.

13. A. Das and M. M. Islam. Securedtrust: a dynamic trust computation model for secured communication in multiagent systems. *IEEE Transactions on Dependable and Secure Computing*. 2012. Vol. 9(2).pp.261–274.

14. S. P. Marsh. *Formalising trust as a computational concept*. 1994.

15. J. R. San Crist´obal. *Multi criteria analysis in the renewable energy industry. Springer Science & Business Media*, 2012.

16. I. F. Akyildiz, B. F. Lo, and R. Balakrishnan. Cooperative spectrum sensing in cognitive radio networks: *A survey. Physical Communication*. 2011. Vol. 4(1).pp.40–62.

17. R. L. Keeney. Utility functions for multiattributed consequences. *Management Science*. 1972. Vol. 18(5-part-1).pp.276–287.

18. J. R. San Crist´obal. Multi criteria analysis in the renewable energy industry. *Springer Science & Business Media*, 2012.

19. R. L. Keeney. Multiplicative utility functions. *Operations Research*. 1974. Vol. 22(1). Pp.22–34.

20. T. Qin, H. Yu, C. Leung, Z. Shen, and C. Miao. Towards a trust aware cognitive radio architecture. *ACM SIGMOBILE Mobile Computing and Communication Review*. 2009. Vol. 13 (2).pp.86 – 95.

21. J. Feng, M. Wang, G. Lu, and J. Li. Trusted cooperative spectrum sensing scheme based on ds evidence theory. *In International Conference on Information and Communications Technologies (ICT 2015)*. 2015. Vol. IET.pp.1–5.

22. Y. Cai, Y. Mo, K. Ota, C. Luo, M. Dong, and L. Yang. Optimal data fusion of collaborative spectrum sensing under attack in cognitive radio networks. *IEEE Network*. 2014. Vol. 28(1).pp.17–23.

23. J. Shlens. Notes on kullback-leibler divergence and likelihood. arXiv preprint arXiv:1404.2000, 2014.

24. G. Holmes, A. Donkin, and I. H. Witten. Weka: A machine learning workbench. *In 02nd Australian and Nw Zealand Conference on Intelligent Information Systems*. 1995. Vol. IEEE.pp.357-361.

25. C. S. Hyder, B. Grebur, L. Xiao, and M. Ellison. Arc: Adaptive reputation based clustering against spectrum sensing data falsification attacks. *IEEE Transactions on Mobile Computing*. 2014. Vol. 13(8).pp.1707–1719.

26. W. Guo, S. Chen, Y. Guo, L. Luo, and Z. Zhao. Truster: Trusted social behavior in- spired scheme for cooperative spectrum sensing. *In 16th International Conference on Communication Technology (ICCT)*. 2015. Vol. IEEE.pp.583–588.

27. N. Wang, N. Zhang, and M. Wang. Wireless sensors in agriculture and food industryrecent development and future perspective. *Computers and electronics in agriculture*. 2006. Vol. 50(1).pp.1–14.

28. A. Pantelopoulos and N. G. Bourbakis. A survey on wearable sensor-based systems for health monitoring and prognosis. *IEEE Transactions on Systems, Man, and Cybernet- ics, Part C (Applications and Reviews)*/ 2010. Vol. 40(1).pp.1–12.

29. J. Wang, R. Chen, J. J. Tsai, and D.-C. Wang. Trust-based cooperative spectrum sensing against ssdf attacks in distributed cognitive radio networks. *In International Workshop Technical Committee on Communications Quality and Reliability (CQR 2016)*. 2016. Vol. IEEE.pp.1–6.

30. H. Hu, H. Zhang, H. Yu, Y. Xu, and N. Li. Minimum transmission delay via spectrum sensing in cognitive radio networks. *In IEEE Wireless Communications and Networking Conference (WCNC)*. 2013. Vol. IEEE.pp.4101–4106.

31. S. D. Nguyen, T.-L. Pham, and D.-S. Kim. Dynamic spectrum handoff for industrial cognitive wireless sensor networks. *In 11th IEEE International Conference on Industrial Informatics (INDIN)*. 2013. Vol. IEEE.pp.92–97.

32. A. J. Goldsmith and P. P. Varaiya. Capacity of fading channels with channel side infor- mation. *IEEE Transactions on Information Theory*. 1997. Vol. 43(6).pp.1986–1992.

33. A. J. Goldsmith and P. P. Varaiya. Capacity of fading channels with channel side infor- mation. *IEEE Transactions on Information Theory*. 1997. Vol. 43(6).pp.1986–1992.

34. A. Leon-Garcia. *Probability and Random Processes for Electrical Engineering*. 2004.

35. A. Wald. On cumulative sums of random variables. *The Annals of Mathematical Statistics*. 1944. Vol. 15(3).pp.283–296.

36. D. R. Cox. Renewal theory, 1962. Vol. 58. Methuen.

37. V. Salmani, S. T. Zargar, and M. Naghibzadeh. A modified maximum urgency first scheduling algorithm for real-time tasks. *Transactions on Engineering, Computing and Technology*. 2005. ISSN 1305. Vol. 5313.Pp.19–23.

38. Q. Li and W. Ba. A group priority earliest deadline first scheduling algorithm. *Frontiers of Computer Science*. 2012. 6(5).Pp.560–567.

39. Y. Zhang, T. Jiang, L. Zhang, D. Qu, and W. Peng. Analysis on the transmission delay of priority-based secondary users in cognitive radio networks. *In International Conference on Wireless Communications Signal Processing (WCSP)*. 2013. Pp.1–6.

40. J. Liebeherr, D. E. Wrege, and D. Ferrari. Exact admission control for networks with a bounded delay service. *IEEE/ACM Transactions on Networking (TON)*. 1996. Vol. 4(6).Pp.885–901.

41. A. K. Mok. Fundamental design problems of distributed systems for the hard-real-time environment. 1983.

42. S.-H. Oh and S.-M. Yang. A modified least-laxity-first scheduling algorithm for real-time tasks. *In 05th International Conference on Real-Time Computing Systems and Applications*. 1998. IEEE. Pp.31–36.

43. Q. Liu, X. Wang, and Y. Cui. Scheduling of sequential periodic sensing for cognitive radios. *In Proceedings of INFOCOM*. 2013. IEEE. Pp. 2256–2264.

44. M. Weichold, M. Hamdi, M. Z. Shakir, M. Abdallah, G. K. Karagiannidis, and M. Ismail. *Cognitive Radio Oriented Wireless Networks: 10th International*

Conference, CROWN-COM, Doha, Qatar. April 21-23, 2015. Revised Selected Papers, Vol. 156.

45. E. U. Weber. Risk attitude and preference. *Wiley Interdisciplinary Reviews: Cognitive Science*. 2010. Vol. 1(1).Pp.79–88.

46. E. U. Weber and R. A. Milliman. Perceived risk attitudes: Relating risk perception to risky choice. *Management science*. 1997. Vol. 43(2).Pp.123–144.

47. S. Schechter. Quantitatively differentiating system security. *In 01st Workshop on Eco- nomics and Information Security*. 2002. Citeseer. Pp.16–17.

48. S. E. Schechter. Toward econometric models of the security risk from remote attacks. *IEEE Security & Privacy*. 2005. Vol. 3(1).Pp.40–44.

49. A. Wool. A quantitative study of firewall configuration errors. *Computer*. 2004. Vol. 37(6).Pp.62–67.

50. J. Kohlrausch. Experiences with the noah honeynet testbed to detect new internet worms. *In Fifth International Conference on IT Security Incident Management and IT Foren- sics (IMF'09)*. IEEE. Pp.13–26.

51. G. Grieco, G. L. Grinblat, L. Uzal, S. Rawat, J. Feist, and L. Mounier. Toward large- scale vulnerability discovery using machine learning. *In Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*. 2016. ACM. Pp.85–96.

52. L. Bilge and T. Dumitras. Before we knew it: an empirical study of zero-day attacks in the real world. *In ACM conference on Computer and communications security, pages*. 2012. Pp.833–844.

53. R. Jensen and Q. Shen. Fuzzy-rough sets for descriptive dimensionality reduction. *In IEEE International Conference on Fuzzy Systems (FUZZ-IEEE'02)*. 2002. Vol. 1.Pp.29–34,

54. A. Almutairi, M. Sarfraz, S. Basalamah, W. Aref, and A. Ghafoor. A distributed access control architecture for cloud computing. *IEEE Software*. 2012. Vol. 29(2).Pp.36 – 44.

55. Gopalakrishnan. Cloud computing identity management. *SETLabs briefings*. 2009. Vol. 7(7).Pp.45–54.

56. A. Ullah, J. Li, A. Hussain, and Y. Shen. Genetic optimization of fuzzy membership functions for cloud resource provisioning. *In IEEE Symposium Series on Computational Intelligence (SSCI)*. 2016. IEEE. Pp.1–8.

57. A. Ullah, J. Li, A. Hussain, and Y. Shen. Genetic optimization of fuzzy membership functions for cloud resource provisioning. *In IEEE Symposium Series on Computational Intelligence (SSCI)*. 2016. IEEE. Pp.1–8.

58. Y. Zhang, T. Jiang, L. Zhang, D. Qu, and W. Peng. Analysis on the transmission delay of priority-based secondary users in cognitive radio networks. *In International Conference on Wireless Communications Signal Processing (WCSP)*. 2013. Pp.1–6.

59. M. G. Dondo. A vulnerability prioritization system using a fuzzy risk analysis approach. *In IFIP International Information Security Conference*. 2008, Springer. Pp.525–540.

60. K. J. Arrow. The role of securities in the optimal allocation of risk-bearing. The Review of Economic Studies, 31(2):91–96, 1964.

61. A. in Cyber Systems and T. G. of MIT. http://www.ll.mit.edu/mission/communications/cyber/CSTcorpo/ideval/data/index.html, 2000. Data downloaded on 16-08-2014.

62. I. V. Kotenko and E. Doynikova. Evaluation of computer network security based on attack graphs and security event processing. *JoWUA*. 2014. Vol. 5(3).Pp.14–29.

63. H. Pardue, J. Landry, and A. Yasinsac. A risk assessment model for voting systems using threat trees and monte carlo simulation. *In Requirements Engineering for e-Voting Systems (RE-VOTE), 2009 First International Workshop on*. 2010. IEEE. Pp.55–60.

64. CVE. Common vulnerabilities and exposures (cve). http://cve.mitre.org/cve/cve.html. 2014.

65. J. V. Cleemput, B. Coppens, and B. De Sutter. Compiler mitigations for time attacks on modern x86 processors. *ACM Transactions on Architecture and Code Optimization (TACO)*. 2012. Vol. 8(4).Pp.23.

66. F. Lombardi and R. Di Pietro. *Secure virtualization for cloud computing. Journal of Network and Computer Applications*. 2011. Vol. 34(4).Pp.1113–1122.

67. M. Godfrey and M. Zulkernine. A server-side solution to cache-based side-channel attacks in the cloud. *In 06th IEEE International Conference on Cloud Computing*. 2013. Pp.163– 170.

68. Y. Zhang, A. Juels, A. Oprea, and M. K. Reiter. Homealone: Co-residency detection in the cloud via side-channel analysis. *In IEEE Symposium on Security and Privacy*. 2011. Pp.313–328.

69. T. Ristenpart, E. Tromer, H. Shacham, and S. Savage. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. *In 16th ACM conference on Computer and communications security*. 2009. ACM. Pp.199–212.

70. S. Sundareswaran and A. C. Squcciarini. Detecting malicious co-resident virtual machines indulging in load-based attacks. *In Information and Communications Security*. 2013. Springer. Pp.113–124.

71. P. Sun, Q. Shen, Y. Chen, Z. Wu, C. Zhang, A. Ruan, and L. Gu. Poster: Lbms: load balancing based on multilateral security in cloud. *In 18th ACM Conference on Computer and Communications security*. 2011. ACM. Pp.861–864.

72. S. Voigt, T. Kemper, T. Riedlinger, R. Kiefl, K. Scholte, and H. Mehl. Satellite image analysis for disaster and crisis-management support. *IEEE transactions on Geoscience and Remote Sensing*, 2007. Vol. 45(6).Pp.1520–1528.

73. S. Roche, E. Propeck-Zimmermann, and B. Mericskay. Geoweb and crisis management: *Issues and perspectives of volunteered geographic information. GeoJournal*. 2013. Vol. 78(1).Pp.21–40.

74. R. Klauck, J. Gaebler, M. Kirsche, and S. Schoepke. Mobile xmpp and cloud service collab- oration: An alliance for flexible disaster management. *In 17th International Conference on Collaborative Computing: Networking, Applications and Worksharing (Collaborate- Com)*. 2011. IEEE. Pp.201–210.

75. D. Puthal, S. Nepal, R. Ranjan, and J. Chen. A secure big data stream analytics frame- work for disaster management on the cloud. *In IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th*

International Confer- ence on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS). 2016. IEEE. Pp.1218–1225.

76. P. Arias-Cabarcos, F. Almenrez-Mendoza, A. Marn-Lpez, D. Daz-Snchez, and R. Snchez- Guerrero. *A metric-based approach to assess risk for on cloud federated identity man- agement. Journal of Network and Systems Management*. 2012. Vol. 20(4).Pp.513–533.

77. S. S. Chow, Y.-J. He, L. C. Hui, and S. M. Yiu. Spice–simple privacy-preserving identity- management for cloud environment. *In Applied Cryptography and Network Security*. 2012. Spirnger. Pp.526–543.

78. L. Yan, C. Rong, and G. Zhao. Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. *In Cloud Computing*. 2009. Springer. Pp.167–177.

79. G. Dreo, M. Golling, W. Hommel, and F. Tietze. Iceman: An architecture for secure federated inter-cloud identity management. *In IFIP/IEEE International Symposium on Integrated Network Management (IM 2013)*. 2013. IEEE. Pp.1207–1210.

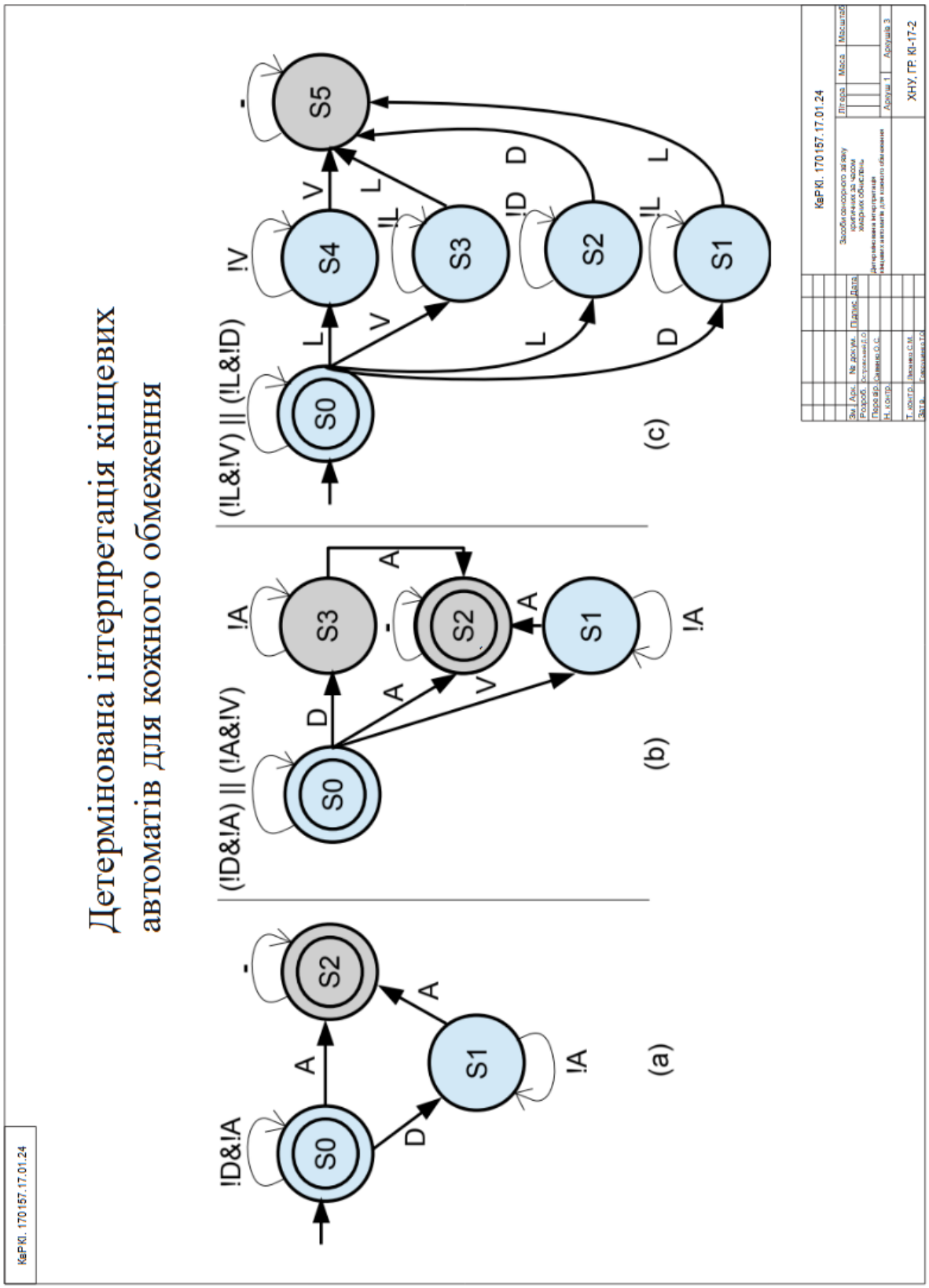
80. P. Arias-Cabarcos, F. Almenrez-Mendoza, A. Marn-Lpez, D. Daz-Snchez, and R. Snchez- Guerrero. *A metric-based approach to assess risk for on cloud federated identity man- agement. Journal of Network and Systems Management*. 2012. Vol. 20(4).Pp.513–533.

81. Z. Quan, S. Cui, and A. H. Sayed. Optimal linear cooperation for spectrum sensing in cognitive radio networks. *IEEE Journal of selected topics in signal processing*. 2008. Vol. 2(1).Pp.28–40.

Додаток А

(обов'язковий)

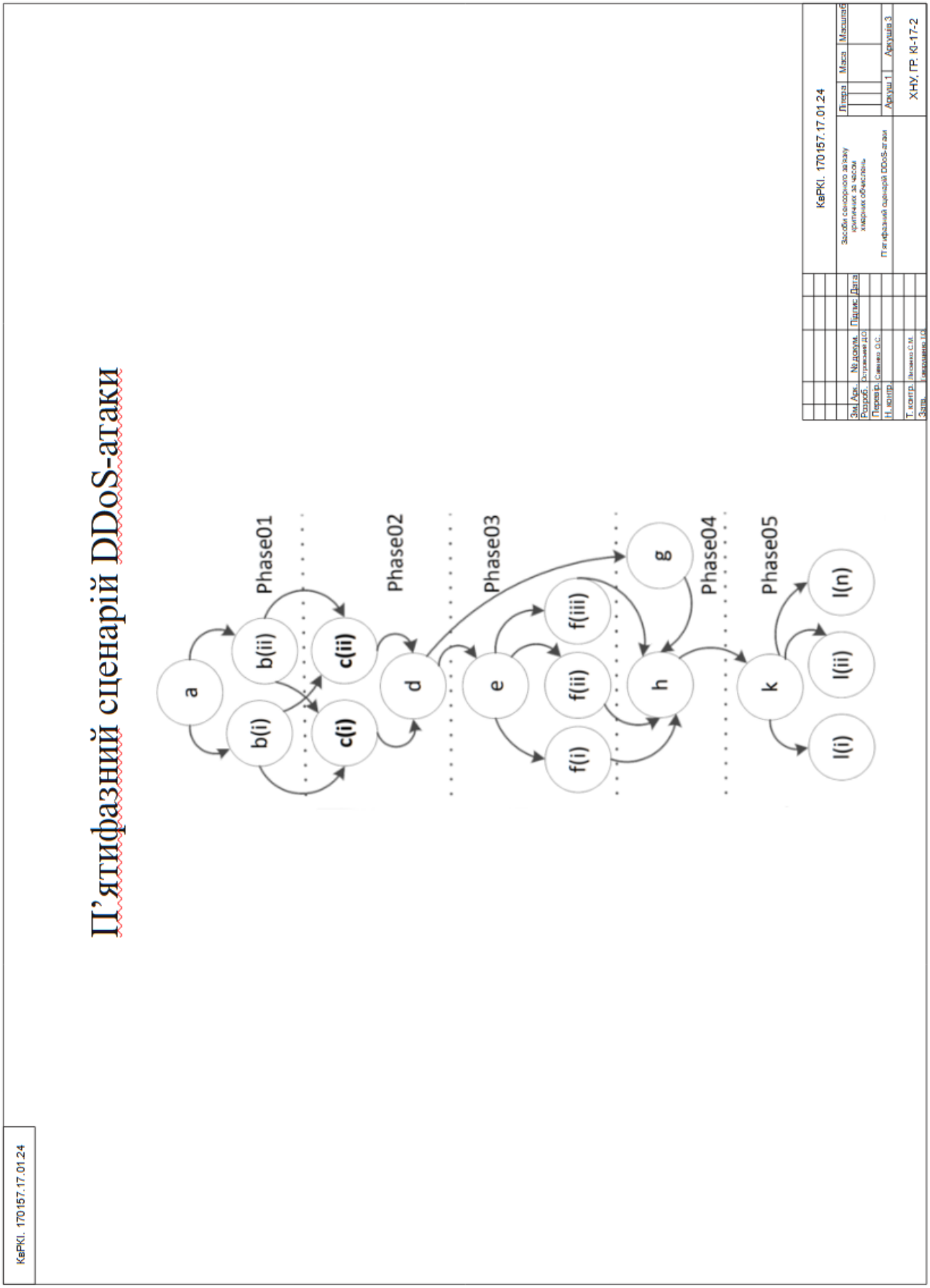
Копія креслення «Детермінована інтерпретація кінцевих автоматів для кожного обмеження: (a) ψr - відповідне обмеження існування, (b) ψp - обмеження переваги та (c) ψn - не обмеження існування»



Додаток Б

(обов’язковий)

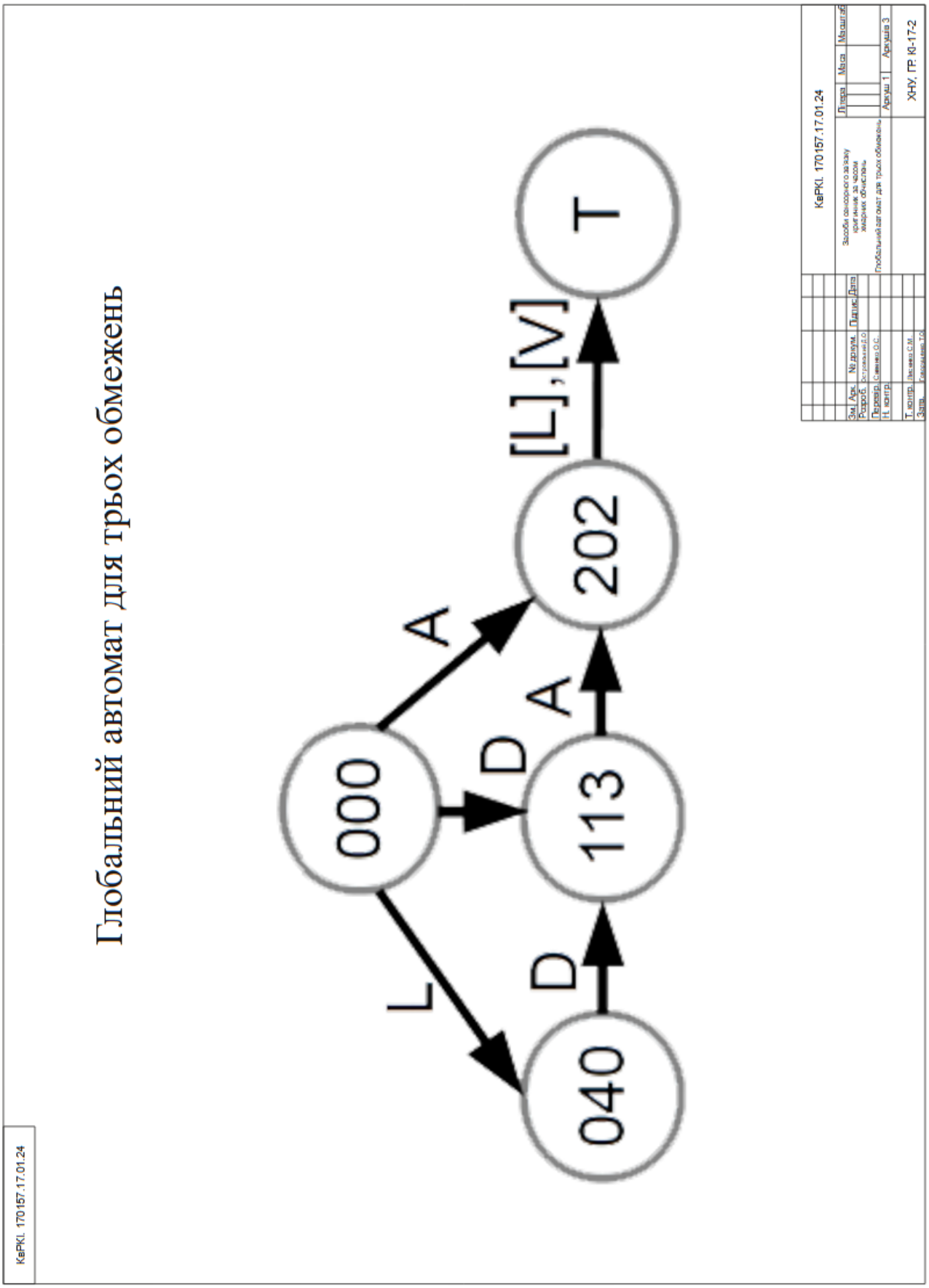
Копія креслення «П’ятифазний сценарій DDoS-атаки»



Додаток В

(обов'язковий)

Копія креслення «Глобальний автомат для трьох обмежень»



UNICHECK

Ім'я користувача:
Кафедра КІ

ID перевірки:
1008324998

Дата перевірки:
18.06.2021 07:05:56 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
18.06.2021 07:06:16 EEST

ID користувача:
100005591

Назва документа: **Островський_Засоби сенсорного зв'язку критичних за часом хмарних обчислень**

Кількість сторінок: **79** Кількість слів: **14049** Кількість символів: **105363** Розмір файлу: **1.15 MB** ID файлу: **1008396614**

13.6%
Схожість

Найбільша схожість: **3.19%** з джерелом з Бібліотеки (ID файлу: **1008214710**)

8.85% Джерела з Інтернету	593	Сторінка 81
5.67% Джерела з Бібліотеки	100	Сторінка 86

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

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

Замінені символи	43

Fri Jun 18 06:18:06 EEST 2021, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 4.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 11%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 94617 Название: Засоби сенсорного зв'язку критичних за часом хмарних обчислень Добавлено в БД: 2021-06-18 Авторы: Д.О. Островський Руководители: О.М. Березький Консультанты: Опоненты:	Символы	Лексемы	Символы	Лексемы
	84702	785	5035 (6%)	57 (7%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник Островський Денис Олексійович
Тема Засоби сенсорного зв'язку критичних за часом хмарних обчислень
Спеціальність 123 Комп'ютерна інженерія

Обсяг кваліфікаційної роботи:

кількість листів креслень 3 ; кількість сторінок записки 80
1. Короткий зміст КП та прийнятих рішень В рамках кваліфікаційної роботи було розроблено засоби сенсорного зв'язку критичних за часом хмарних обчислень

2. Висновок про відповідність КП дипломному завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині.
3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому, теоретичному, розділі кваліфікаційної роботи якісно та в повній мірі розглянуті методи вирішення поставленої задачі, був проаналізований кожен аспект, який стосується теми кваліфікаційної роботи. У наступному розділі було проведено порівняльну характеристику модулів, що можуть використовуватись в системі. Рішення про використовувані модулі обґрунтовано. Також були розглянуті переваги та недоліки засобів зв'язку. У основній проектній частині роботи була реалізована сучасними методами та рішеннями система багатоатрибутних довір. За проведеним у попередніх розділах аналізом, систему було покращено. Було проведено тестування системи у двох варіантах – класичного вигляду, та покращеного. В загальному усі розділи відповідають завданню та містять сучасні методи вирішення поставлених завдань.
4. Позитивні сторони проекту Кваліфікаційна робота відповідає сучасним вимогам до проектування мультипроцесорних систем. Для проектування системи були використані сучасні програмно-апаратні рішення.

5. Негативні сторони проекту Недостатня деталізація в плані прикладної розробки засобів. Добре було б детальніше розглянути питання масштабованості та організації системи.

6. Оцінка графічного оформлення та пояснювальної записки проекту Графічне оформлення виконане відповідно до суті кваліфікаційної роботи. У першому листі відображено детермінована інтерпретація кінцевих автоматів для кожного обмеження відповідно до теми. У другому листі показано п’ятифазний сценарій DDoS-атаки. Третій лист представляє собою глобальний автомат для трьох обмежень відповідно до теми роботи. В загальному графічне оформлення виконане на належному рівні. Пояснювальна записка відповідає задекларованим нормам для її оформлення.

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує схвалення. Основна частина роботи структурована. Графічний матеріал дозволяє побачити основні аспекти надійності засобів сенсорного зв’язку відповідно до змісту роботи та методи покращення існуючих рішень для засобів сенсорного зв’язку критичних за часом хмарних обчислень.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Розглянувши позитивні та негативні сторони представленого дипломного проекту, можна зробити висновок, що він заслуговує оцінку «задовільно»

РЕЦЕНЗЕНТ (прізвище, ім’я, по батькові, посада, місце роботи) доцент кафедри автоматизації, комп’ютерно-інтегрованих технологій та телекомунікацій, к.т.н. Федула Микола Васильович

« _____ » _____ 2021 р. _____ (підпис)

ХНУ. Зам. 54, тир. 6000, 2007.

Завідувачу кафедри КІСП
д-р.техн.наук, проф. Говорущенко Т. О.

Островський Денис Олексійович
ПІБ здобувача вищої освіти

ФПКТС, 4 курсу, групи КІ-17-2

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 29.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіатоповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

_____ _____

дата підпис

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА СИСТЕМНОГО ПРОГРАМУВАННЯ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Засоби сенсорного зв'язку критичних за часом хмарних обчислень

Автор: Островський Денис Олексійович

Спеціальність: 123 – Компютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Савенко О.С.

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих засобів та обмежень існуючих засобів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні;
3) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з більш ніж 10 джерелами на один фрагмент речення;
4) серед запозичень знаходяться загальновідомі терміни, скорочення та визначення.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 13.6% і адресується до 693 першоджерела, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ О.С. Савенко

Гарант ОП _____ С.М. Лисенко

Завідувач кафедри КІСП _____ Т. О. Говорущенко