Всеукраїнський конкурс студентських наукових робіт

Комп’ютерна інженерія

СТУДЕНТСЬКА НАУКОВА РОБОТА

На тему: ***«Технологія віддаленого керування науковими інструментами на платформі оверлейних мереж»***

Шифр: ***«Віддалений доступ»***

2020

ЗМІСТ

ВСТУП

Українська наука отримала у спадок від Радянського Союзу велику кількість наукових інструментів (наприклад, радіоастрономічні та оптичні обсерваторії, системи спостереження за станом земної кори тощо) [1]. Але через те, що більша їх частина мала подвійне призначення, вони були здебільшого ізольовані від потужних центрів обробки даних, а, власне, дані доставлялися для аналізу за допомогою фізичних носіїв [2].

Вихід України з радянського блоку та інтеграція її в світову дослідницьку мережу у поєднанні з стрімким розвитком інформаційних технологій дозволило показати цінність наукових інструментів для іноземних партнерів для їх заохочення інвестувати в розвиток цих наукових інструментів [3]. Інформаційні технології дали змогу не лише зберігати великі обсяги даних та мати можливість миттєвого доступу до них, а й здійснювати безпосередню підтримку в процесах моніторингу ряду показників та керування науковим обладнанням.

Як говорилося раніше, прикладом таких систем є системи моніторингу показників віддалених астрономічних станцій з телескопами, сейсмічних станцій контролю та реєстрації коливань земної поверхні, що викликаються землетрусами для прогнозування та передвчасної евакуації населення, станції моніторингу рівня екологічної небезпеки, температури, прогнозування штормів, також контроль внутрішніх вод для моніторингу режиму паводків та повені тощо. Спільною рисою цих систем є віддаленість від населених пунктів з метою мінімізації впливу перешкод від побутових приладів, антропогенного чинника, електромагнітного забруднення.

Таким чином, оперативне отримання інформації з вищенаведених систем стикається з двома проблемами: безпечна передача цінних даних від системи реєстрації даних до системи обробки; та інструментарій для віддаленого керування (додаткового налаштування, реконфігурації) науковими інструментами. Це породжується відсутністю безпечних і високошвидкісних

каналів зв'язку у таких віддалених місцях функціонування вищезазначених систем та необхідність створювати власні програмні продукти для дистанційного доступу до модулів управління наукових інструментів, які здебільшого мають нестандартизовані інтерфейси керування. Виходячи з практичного досвіду, найчастіше мережний доступ здійснюється тільки через існуючі відкриті мобільні мережі різних операторів зв'язку [4, 5].

Парадокс української фундаментальної науки полягає у консервативних підходах до вирішення супутніх задач, які є забезпечуючими при вирішенні більш важливих проблем. Наприклад, якщо необхідно виконати наукові дослідження з метою реєстрації деяких космічних явищ, які виникають неперіодично, але мають протяжність у часі 10-15 с, система-реєстратор отримавши дані про явище може сповістити інші системи подібного класу для цільової вказівки для реєстрації цього явища ними з синхронізацією часових відміток (важлива проблема). Важлива роль у цьому лежить на каналах зв’язку, які здебільшого є нестабільними або незахищеними (супутня задача). Як правило, успішність вирішення цієї супутньої задачі є причиною отримання або втрати пріоритету у відкритті нового явища і т.д.

Таким чином, актуальною є науково-прикладна задача створення технології віддаленого керування науковими інструментами, яка б базувалася на застосуванні комп’ютерних мереж, які функціонують поверх існуючих небезпечних мережних інфраструктур операторів мобільного, фіксованого або супутникового зв'язку. Такі мережі називаються оверлейними комп’ютерними мережами.

Метою даної роботи є розробка технології віддаленого керування науковими інструментами на базі оверлейних комп’ютерних мереж, яка включає побудову віртуальних та вкладених багатошарових тунелів. Також в рамках виконання роботи необхідно провести дослідження стабільності функціонування конкретного рішення на базі технології віддаленого керування.

1. ПОСТАНОВКА ЗАДАЧІ

В загальному вигляді задача сформульована як: створення технології віддаленого керування науковими інструментами. Для вирішення цієї задачі необхідно ввести додаткові умови та виконати декомпозицію задачі:

- технологія має передбачати керування віддаленими науковими інструментами через комп’ютерну мережу Інтернет;

- канал зв’язку типу «остання миля» може бути представленим як сегмент комп’ютерних мереж операторів мобільного, фіксованого або супутникового зв'язку (гетерогенна мережа);

- реалізація технології має базуватися на некомерційних програмних продуктах або з мінімальними фінансовими затратами;

- віддалені пристрої наукових елементів можуть містити лише USB-інтерфейси, без мережних інтерфейсів;

- технологія має забезпечувати безпечні умови передачі інформації в гетерогенному мережному середовищі.

2. ОГЛЯД АНАЛОГІЧНИХ РІШЕНЬ

У якості вирішення подібного класу задач, частіше за все використовується програмне забезпечення WireGuard, яке включено до ядра Linux [6]. Його перевага в гнучкості налаштування для створення оверлейної мережі. Дане ПЗ дозволяє створювати Ethernet-тунель поверх L3-тунелю за допомогою технології GRE [6]. Недоліком є те, що при перезавантаженні клієнтських маршрутизаторів, налаштованих для використання цього ПЗ, часто не вдається підключатися до VPN-серверу. Це пояснюється тим, що WireGuard інколи створює маршрут з неправильними інтерфейсами. Це в свою чергу вимагає пошуку додаткових рішень як то: перевірка маршрутів та виконання додаткових скриптів видалення зайвих маршрутів, примусове перевантаження тощо. А в умовах, коли альтернативний доступ до комп’ютерної мережі, де

функціонує науковий інструмент, відсутній, – є ймовірність повної втрати віддаленого доступу.

В роботі [7] розглядається одне з найбільш простих і популярних комерційних рішень – програмне забезпечення Team Viewer – як рішення для віддаленого керування комп'ютером. В цій роботі автори наводять сценарії його застосування і переваги для дистанційного керування, організації загального доступу до робочого столу, для передачі файлів між комп'ютерами тощо.

У якості недоліків використання Team Viewer варто зазначити: так як програмний продукт є комерційним, можуть виникнути проблеми з використанням безкоштовної версії користувачами для вирішення довготермінових задач; є проблема динамічної зміни якості зображення віддаленого робочого столу; програмне забезпечення не кросплатформне; в якості середовища передачі даних використовується мережна інфраструктура з проміжними комунікаційними вузлами компанії-власника Team Viewer, що знижує безпеку в цілому. Таким чином, ПЗ Team Viewer підходить в якості засобу моніторингу робочого столу віддаленого комп'ютера.

Існує ряд інших комерційних рішень, заснованих на використанні оверлейних технологій. Наприклад, рішення LogMeIn Hamachi [8] , що дозволяє створювати різні оверлейні топології мережі . Програма захищає підключення за допомогою 256-бітного шифрування AES і протоколів безпеки. Однак адміністратори з боку компанії-постачальника сервісу також можуть керувати налаштуваннями мережі, надаючи повний, обмежений або мінімальний доступ до функцій користувачам. Також серед недоліків важливо відзначити складності при налаштуванні внутрішньої маршрутизації між вузлами і досить високі економічні витрати.

Відомим є рішення [9], коли функціонал керування віддаленим мікроконтролером можна виконати у вигляді веб-серверу. В цьому випадку, при відсутності реальної IP-адреси для прямого підключення клієнта до пристрою, – необхідно між браузером клієнта і віддаленою системою управління науковим інструментом встановити проміжний веб-сервер, який

здатний виконувати скрипти мовою PHP. В роботі [9] розглянуто приклад, який можна інтерпретувати для нашої задачі у наступному вигляді. Припустимо, один з компонентів системи управління науковим інструментом реалізований за допомогою мікроконтроллера, який працює як веб-клієнт і кожні 10 секунд зчитує значення командного html-файлу. Припустимо, якщо перша позиція файлу дорівнює «-1» , то мікроконтроллер запускає кожні 2 секунд на веб-сервері php- файл і повідомляє йому через параметри стан виконання команди системою управління науковим інструментом. В цьому випадку мікроконтролер звертається до сервера кожну 1 секунду. Виконання будь-якої команди від користувача виконається не пізніше ніж через 2 секунди при ідеальній роботі веб-сервера і каналу зв'язку .

Недоліком даного рішення є можливі обмеження на число звернень до веб-сервера протягом 24 годин. Наприклад, для середньостатистичного хостингу щодобове число звернень не перевищує 10000 раз. Тому мікроконтролер може виконувати не частіше одного звернення за 8 секунд для запобігання блокування хостингом. Існують і інші обмеження, пов'язані з безпекою передачі команд управління через вузли-посередники, так як в більшості з них питання безпеки при проміжному зберіганні можуть не розглядатися зовсім.

3. РОЗРОБКА МЕТОДУ

В основі методу організації віддаленого доступу лежить використання рішення VPN-тунелювання [10]. Для початку необхідно скласти типову схему комп'ютерної мережі. Так, розглянемо комп’ютерну мережу, яка складається з трьох компонентів.

У якості першого компоненту розглянемо сегмент комп’ютерної мережі наукового інструменту, який складається з k обчислювальних станцій. Нехай до однієї з цих станцій (k_1) підключено телекомунікаційне обладнання, що забезпечує низькошвидкісний канал зв'язку з мережею Інтернет (наприклад,

3G-модем). Підсистема керування науковим інструментом з наявним мережним інтерфейсом може бути підключена до комутатора (як і обчислювальні станції). У разі його відсутності, а за наявності USB-інтерфейсу, підключення наукового інструменту може здійснюватися до іншої обчислювальної станції (k_2). За таких умов обчислювальна станція (k_1) функціонує в режимі шлюзу для інших учасників мережі наукового інструменту, забезпечуючи їм доступ до мережі Інтернет (за необхідності).

Другим компонентом є провайдер телекомунікаційних послуг, що надає реальні IP-адреси за технологією VPN.

Третім компонентом є, власне, обчислювальний пристрій користувача, підключений до мережі Інтернет. Метою користувача є отримання доступу до системи управління науковим інструментом через комп'ютерну мережу та/або через віртуальний (емульований) USB-інтерфейс.

Для створення оверлейной мережної інфраструктури для організації віддаленого керування науковим інструментом пропонується наступна послідовність дій.

Крок 1. Необхідно здійснити налаштування делегації реальної IP-адреси шляхом організації окремого VPN-сервера. Для цього можна використовувати стандартні рішення з використанням протоколу PPTP. Так як мова йде тільки про підзадачу видачі адреси, а процеси передачі даних (команд управління тощо) з боку наукового інструменту здійснюватися не будуть, враховуючі останні тенденції в галузі криптостійкості протоколів шифрування, що забезпечують функціонування PPTP, – можна зупиниться саме на цьому рішенні. В іншому випадку можна використовувати більш криптостійкі рішення, наприклад, OpenVPN.

Крок 2. У комп'ютерній мережі, де функціонує науковий інструмент, на обчислювальній станції (k_1), який має доступ до мережі Інтернет через низькошвидкісний канал зв'язку, необхідно інсталювати клієнтське програмне забезпечення для створення VPN-тунелю. Так як оператори мобільного зв'язку, надаючи доступ до мережі Інтернет, як правило, видає кінцевим користувачам

приватні (внутрішні) IP-адреси, то, підключаючись по віртуальному каналу зв'язку до VPN-серверу, налаштованому раніше, обчислювальна станція (k_1) отримує реальну IP -адресу.

Крок 3. Тепер на обчислювальній станції (k_1) необхідно інсталювати VPN-сервер. Цей сервер буде приймати вхідні запити по інтерфейсу, якому присвоєно реальну IP-адресу, отриману згідно попереднього кроку, а IP-адреси, які будуть присвоюватися користувачам, виділяються з пулу адрес внутрішньої комп'ютерної мережі наукового інструменту. У якості програмного VPN-серверу можна використовувати програмне забезпечення OpenVPN, виконуючи умови по безпеці віртуальних з'єднань.

Крок 4. Зі сторони користувача необхідно інсталювати клієнтську частину VPN-тунелю. При підключенні до серверу мережі наукового інструменту, користувацька обчислювальна станція буде приєднуватися по віртуальному каналу до внутрішньої комп'ютерної мережі наукового інструменту.

Виходячи з того, що кількість одночасних підключень до VPN-серверу в комп'ютерній мережі наукового інструменту не обмежується одним, потрібно виконати оцінку стану пропускної здатності віртуального каналу передачі даних між кожним клієнтом і VPN-сервером. Це необхідно для створення підсистеми балансування пропускної здатності в разі нестабільності каналу зв'язку (тобто вирішується підзадача дефіциту ресурсу).

Для оцінки стану пропускної здатності віртуального каналу зв'язку необхідно, щоб всі приграничні маршрутизатори (а при використанні проміжних вузлів – і їх також) користувачів передавали спеціальні пакети даних VPN-серверу, що знаходиться в мережі наукового інструменту [11]. Загальну пропускну здатність тунелю окремо взятого підключення до комп'ютерної мережі обсерваторії через VPN-тунель можна обчислити аналітично відносно з'єднання «точка-точка» за формулою [12]:

$$\Psi = D\ell(2S + (2i-1)\sum_{i=1}^{log_2 S} 2^{i-1}, \quad (3.1)$$

де: D – кількість проміжних маршрутизаторів (в тому числі віртуальних); S – кількість пригранічних маршрутизаторів; ℓ – кількість користувачів, які підключаються до VPN-серверу.

Якщо в комп'ютерній мережі наукового інструменту блок керування, підключений до мережі, генерує широкомовні дані, наприклад, відправляючи моніторингову інформацію для всіх учасників мережі, у тому числі і підключених по VPN-тунелю, – загальна пропускна здатність може бути представлена у вигляді:

$$\Psi' = D(1 + log_2 S + \sum_{i=1}^{log_2 S} 2^i + \ell S), \quad (3.2)$$

В результаті, для розглянутого прикладу комп'ютерної мережі, яка складається з трьох сегментів, значення пропускної здатності, яка неефективно використовується під час передачі від кожного з користувачів, підключених по VPN-тунелю, можна визначити як:

$$\theta = D(\ell S - YW), \quad (3.3)$$

де: Y – середня кількість вершин оверлейної мережі, яка залежить від кількості маршрутизаторів при організації транспорту трафіку через реальні IP-адреси; W – кількість гілок дерева маршрутизації в каскадних схемах підключення [11].

4. ПРОТОТИП ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ ТЕХНОЛОГІЇ

У якості орієнтиру при описі прототипу інформаційно-комунікаційної технології (ІКТ), який було отримано в результаті вирішення науково-

прикладної задачі організації віддаленого керування науковими інструментами на платформі оверлейних мереж, було використано наступне визначення ІКТ: «цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування» [13].

У якості інструментарію доцільно використати UML-діаграму комунікації (рисунок 4.1), на якій зображені взаємодії між вищезгаданими компонентами композитної структури комп’ютерної мережі. На даній діаграмі комунікації вказують на взаємодію між вузлами мережі відповідно до запропонованого методу для організації доступу до наукового інструменту через віртуальні канали зв’язку, незалежно від місця їх розташування. При цьому час як окремий вимір не використовується.

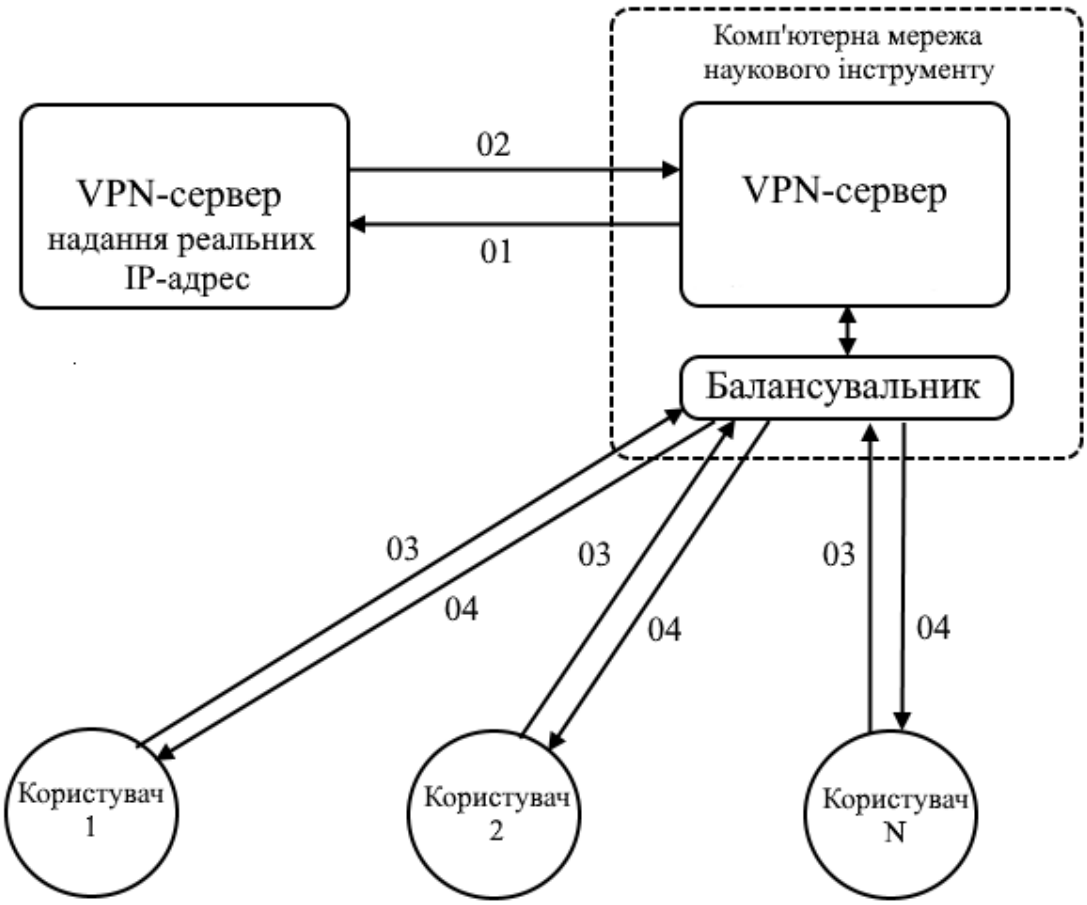

Рисунок 4.1 – UML-діаграма комунікації

Діаграма комунікації моделює взаємодії між вузлами в термінах впорядкованих повідомлень, тобто тут представлено комбінацію інформації, взятої з алгоритму і варіантів використання, описуючи відразу і статичну структуру і динамічну поведінку комп’ютерної мережі в цілому. Зв'язок 01 показує запит обчислювальної станції (k_1) на реальну IP-адресу, а зв'язок 02 – успішну відповідь та видачу такої адреси по віртуальному з’єднанню. Зв'язки 03 та 04 показують відповідні запити та відповіді від користувача до обчислювальної станції (k_1), на якій розгорнуто оверлей з інтерфейсом на базі отриманої реальної IP-адреси.

Так як комунікаційні діаграми характеризуються вільним форматом упорядкування об'єктів і зв’язків, то для підтримки порядку повідомлень при такому вільному форматі, їх хронологічно нумерують. На рисунку не вказано, але всім діям передує перевірка з’єднання комп’ютерної мережі наукового інструменту з мережею Інтернет; послідуюча нумерація триває по напрямку пересилання повідомлень від вузла до вузла.

5. ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ

Експериментальні дослідження базової та ряду модифікацій (в залежності від додаткових умов задачі) технології проводяться з 2015 р. Автор роботи бере безпосередню участь у постановці експериментів та розробці модифікованих прикладних рішень з організації віддаленого доступу до наукових інструментів з грудня 2016 року.

Так, у 2015-2017 рр. була поставлена задача організації віддаленого керування блоком керування радіотелескопом УТР-2 і здійснення доступу до локальної обчислювальної станції збору моніторингової інформації, що знаходяться в Радіоастрономічної обсерваторії ім. С.Я. Брауде (РАО) Радіоастрономічного інституту НАН України [14]. Додатковими умовами задачі були: комп'ютерна мережа РАО підключена до мережі Інтернет за допомогою обчислювальної станції-шлюзу, яка в свою чергу підключена до 3G-

модему; Інтернет-провайдер не надає виділених реальних IP-адрес; канал зв'язку може бути нестійким при складних кліматичних або електромагнітних умовах (сніг, туман, дощ, магнітна буря і т.д.); доступ до локальної обчислювальної станції і блоку керування повинен бути захищеним, авторизованим і надаватися відповідно до заздалегідь затвердженого графіку виконання робіт. Також вводиться вимога до розділу віддалених користувачів на два класи: користувачі, які можуть завантажувати завдання блоку керування (через спеціалізоване програмне забезпечення), відправляючи команди через комп'ютерну мережу і спостерігати за виконанням спостережень на своїй обчислювальній станції (в цьому випадку обчислювальна станція носить назву дистанційно-керуюча); і користувачі, які можуть завантажувати завдання з локальної обчислювальної станції комп'ютерної мережі РАО і періодично перевіряти їх виконання через інтерфейс локально обчислювальної станції.

Виходячи з вищесказаного, умовно задачу можна розбити на кілька підзадач: організація зовнішнього інтерфейсу комп'ютерної мережі РАО для можливості підключення користувачів з мережі Інтернет з метою безперервної взаємодії з блоком керування; і організація віддаленого доступу до локальної обчислювальної станції РАО з метою локальної постановки задачі і моніторингу виконання роботи блоку керування радіотелескопом. Так як блок керування радіотелескопом може взаємодіяти з локальною обчислювальною станцією РАО, яка знаходиться в одноранговій мережі, обчислювальна станція користувача повинна мати IP-адресу з підмережі РАО.

В даному випадку була використана запропонована вище технологія організації віддаленого доступу. Одна з обчислювальних станцій комп'ютерної мережі РАО була налаштована в ролі VPN-сервера. Однак, так як мобільний Інтернет-провайдер не мав можливості надати реальну IP-адресу, було прийнято рішення отримувати таку IP-адресу з комп'ютерної мережі РІ НАНУ (в розпорядженні РІ НАНУ є пул (256) реальних IP-адрес, тому є технічна можливість надання реальної IP-адреси за допомогою інсталяції VPN-сервера).

Тепер обчислювальна станція-шлюз комп'ютерної мережі РАО, підключаючись до VPN-серверу РІ НАНУ отримує реальну IP-адресу. Далі була вирішена зворотна задача, коли на обчислювальній станції-шлюзі комп'ютерної мережі РАО встановлено VPN-сервер, у якого в якості інтерфейсу для підключення використовується реальна IP-адреса, отримана від VPN-серверу РІ НАНУ.

Користувач, підключаючись до VPN-серверу в РАО за реальною IP-адресою, отримує внутрішню IP-адресу комп'ютерної мережі РАО. Таким чином, обчислювальна станція користувача може виконувати роль дистанційно-керуючої, маючи можливість відправляти і приймати дані з блоку керування радіотелескопом. Схематично структура оверлейної мережі буде мати такий вигляд (рисунок 5.1) .

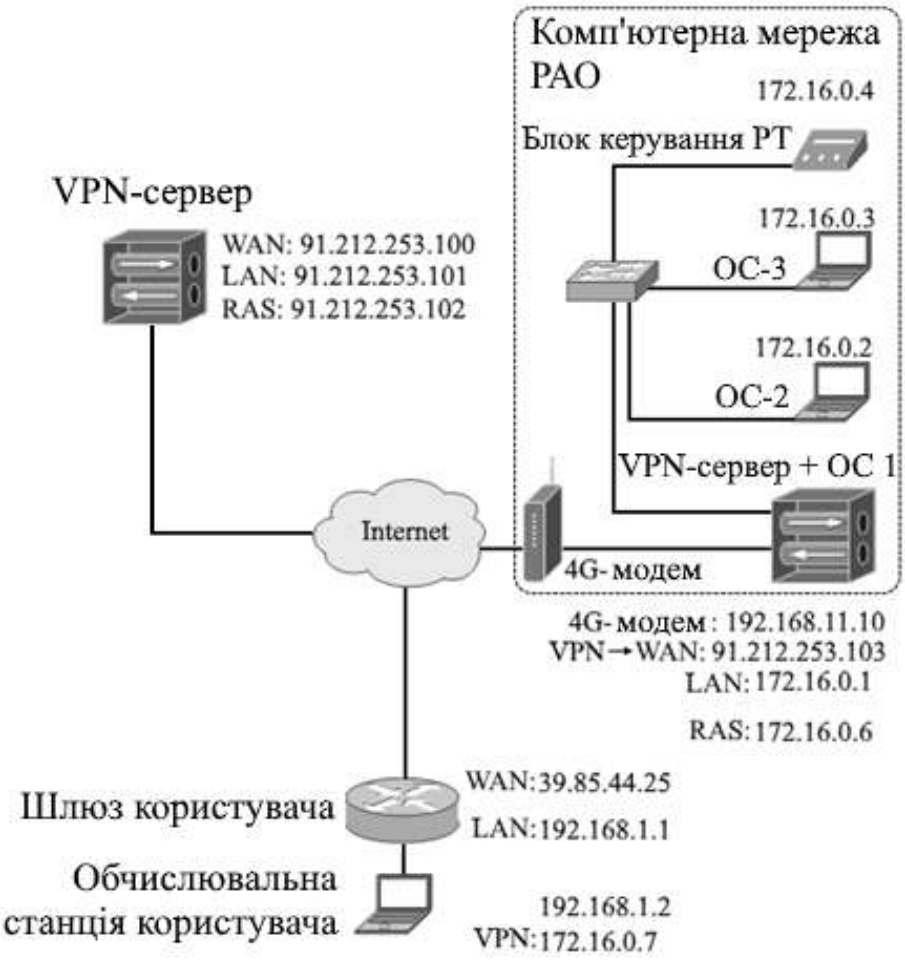

Рисунок 5.1 – Технологія реалізації віддаленого керування блоком управління радіотелескопом УТР-2 в РАО ім. С.Я. Брауде РІ НАНУ

Основні проблеми даної реалізації полягають в залежності коректної роботи задіяних сервісів з тунелювання від нестійкого Інтернет-каналу в РАО. У разі розриву з'єднання Інтернет-провайдером, обчислювальна станція-шлюз робить процедуру повторного підключення до VPN-серверу РІ НАНУ. Цей алгоритм виконує і дистанційно-керуюча обчислювальна станція. І хоча після відправки команд керування на блок керування радіотелескопом, останній їх виконує, то при відсутності зв'язку між учасниками мережі, звіт про виконання команди, звісно, не надходить вчасно. Тому, при тривалих радіоастрономічних онлайн-спостереженнях (більше 10 годин) недоцільно використовувати вищевказаний підхід. Досить завантажити команди управління на локальну обчислювальну станцію РАО і періодично перевіряти виконання завдання спостереження за допомогою підключення до робочого столу локальної обчислювальної станції РАО відомими способами.

У 2019 у зв'язку з модернізацією апаратного комплексу керування радіотелескопом та введенням в експлуатацію системи віддаленого керування новим радіотелескопом ГУРТ (Гігантський Український Радіотелескоп) РАО РІ НАНУ, виникла необхідність організації віддаленого керування деякими модулями, підключеними за допомогою USB-інтерфейсу до однієї з обчислювальних станцій. Для цього був розроблений прототип рішення, заснований на використанні програмного забезпечення (ПЗ) проекту USB/IP. Це ПЗ дозволяє здійснювати обмін даними з USB-пристроями через локальну мережу та призначено для спільного використання USB-пристроїв між обчислювальними станціями. При повному збереженні функціоналу ПЗ USB/IP трансформує «USB I/O повідомлення» в TCP/IP дані, які можна зчитати, і передає їх між обчислювальними станціями.

Загальним в цих модифікаціях розробленої технології залишається те, що для мережі з низькошвидкісним зовнішнім каналом зв’язку через VPN-тунель завжди виділяється декілька реальних IP-адрес з РІ НАНУ. Однак це не завжди може бути можливим. Наприклад, якщо відсутній з деяких причин доступ до мережі РІ НАНУ, де знаходяться серверні потужності, у тому числі і VPN-

сервер, то необхідно використати резервну схему підключення з використанням однієї IP-адреси допоміжного провайдеру. Тобто в наявності є лише одна реальна IP-адреса на допоміжному майданчику. В такому випадку мови про надання виділеного адреси віддаленого сегменту мережі може і не йти. В такому випадку пропонується наступне технічне рішення (рисунок 5.2).

Рисунок 5.2 – Організація оверлейної мережевої архітектури в разі єдиної реальної IP -адреси

У цьому випадку на приграничному маршрутизаторі резервного майданчика необхідно виконати перенаправлення забезпечуючих портів для того, щоб VPN-сервер був доступний для підключення. Обчислювальна станція (k_1), що знаходиться в комп'ютерній мережі РАО, при підключенні до такого VPN-серверу буде отримувати приватну (сіру) IP-адресу. Для підключення до

VPN-серверу у комп'ютерній мережі РАО необхідно для отриманої приватної IP-адреси виконати перенаправлення портів на шлюзі резервного майданчика, які забезпечують підключення до VPN-сервера в комп'ютерній мережі РАО.

Тепер користувач, в налаштуваннях VPN-підключення вказує IP-адресу шлюзу 109.86.225.127. Запит по заданому порту буде переадресовано по віртуальному тунелю вузлу 10.24.33.33, який в свою чергу видасть користувачу IP-адресу з комп'ютерної мережі обсерваторії. Тут достатньо прописати маршрут підмережі 172.16.0.0/24 через шлюз мережі обсерваторії для встановлення видимості сегменту мережі по віртуальному з'єднанню користувачем.

Іншою задачею експериментального дослідження було визначення оптимального схеми використання протоколу UDP для передачі інформації по захищеним SSL-VPN-тунелям, реалізованим із застосуванням програмного забезпечення OpenVPN (якщо основний тунель налаштований на роботу з TCP, сервер буде отримувати TCP-пакети OpenVPN, які містять інші TCP-сегменти від клієнта. У результаті в ланцюзі виходить подвійна перевірка на цілісність інформації, що абсолютно не має сенсу, тому що надійність не підвищується, а швидкість передачі даних знижується). Було проведено дослідження залежності швидкості передачі команд керування на блок керування радіотелескопом ГУРТ від ймовірності втрати пакетів в мережі при застосуванні протоколу UDP. Згідно відомої методики постановки подібних експериментів [15, 16], експеримент був побудований на тестуванні тунелювання UDP поверх UDP. Даний експеримент проводився для всіх віртуальних тунелів згідно схеми оверлейної мережі (рисунок 5.2).

Вихідні дані для проведення експерименту: розмір пакетів, переданих на блок керування радіотелескопом – 65520 байт; розмір пакетів, що передаються з блоку керування радіотелескопом – 8001 байт; співвідношення інтенсивності передачі відправлених і прийнятих пакетів – 1/10. Експеримент проводився двічі: 01 вересня 2019 року (результати відображені у публікації [12]) та 05

січня 2020 року в Радіоастрономічної обсерваторії ім. С.Я. Брауде Радіоастрономічного інституту НАН України.

Результати експерименту від 05 січня 2020 року по тунелюванню маршруту «Користувач»-«Комп'ютерна мережа обсерваторії» при відправці команд керування блоку керування радіотелескопом ГУРТ з використанням схеми тунелювання по UDP і по TCP представлені в таблиці 5.1 та на рисунку 5.3.

Таблиця 5.1 – Результати експерименту від 05 січня 2020 р.

№ п/п	Імовірність відкидання пакетів, %	Інтенсивність, пакет/с	Кількість втрачених пакетів, шт.
Використання схеми тунелювання по UDP			
1	0	50	0
2	2	100	2
3	4	150	1
4	6	200	4
5	8	250	11
6	10	300	21
Використання схеми тунелювання по TCP			
1	0	50	0
2	2	100	1
3	4	150	1
4	6	200	2
5	8	250	6
6	10	300	6

У порівнянні з результатами експерименту від 01 вересня 2019 р. (результати відображені у публікації [12]) спостерігається стабільність за кількістю втрачених пакетів.

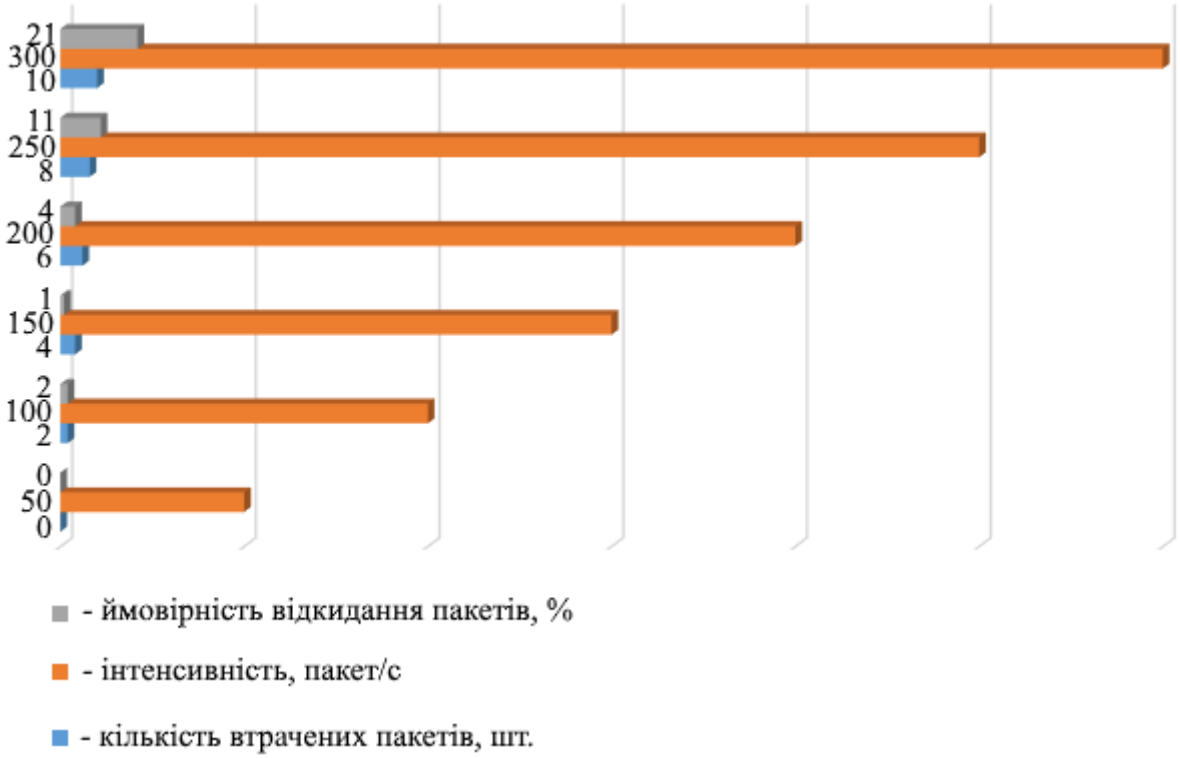

Рисунок 5.3 – Результати експерименту від 05 січня 2020 р. при відправці команд керування

У таблиці 5.2 та на рисунку 5.4 представлені результати експерименту від 05 січня 2020 р. при дослідженні втрат пакетів при прийомі моніторингової інформації з блоку керування радіотелескопом користувачем.

Таблиця 5.2 – Результати експерименту від 05 січня 2020 р.

№ п/п	Імовірність відкидання пакетів, %	Інтенсивність, пакет/с	Кількість втрачених пакетів, шт.
1	0	50	1
2	2	100	6
3	4	150	11
4	6	200	36
5	8	250	44
6	10	300	52

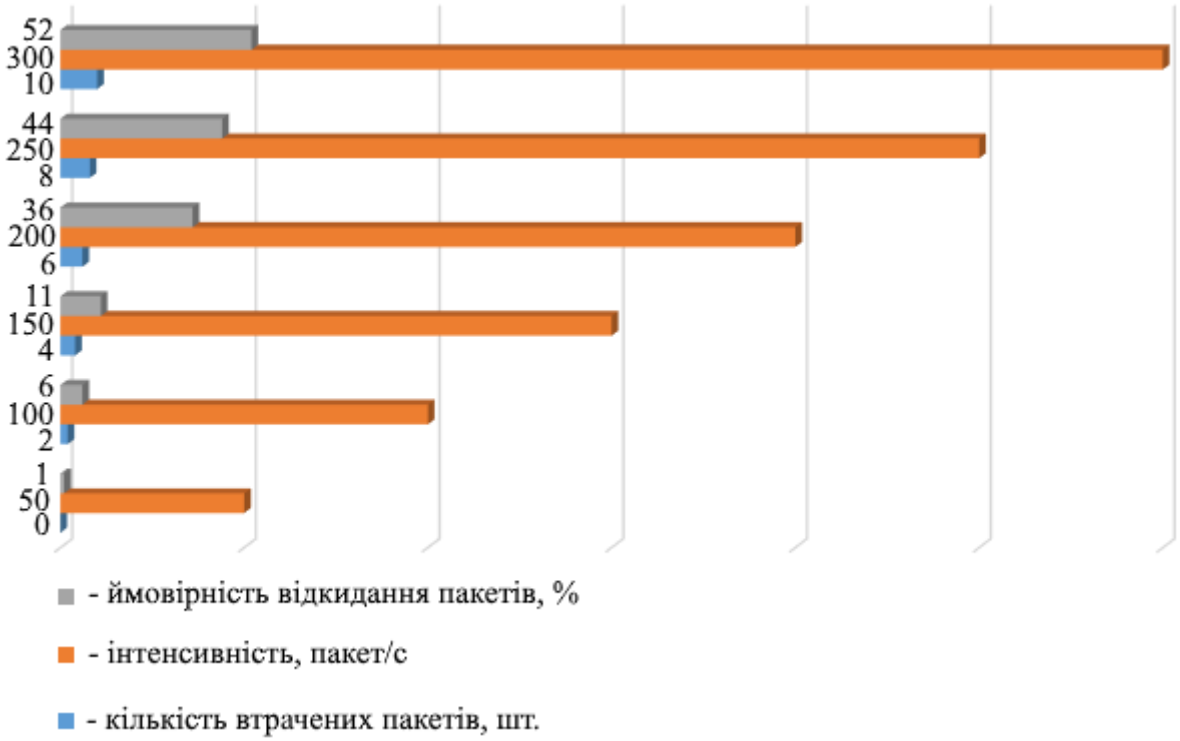

Рисунок 5.4 – Результати експерименту від 05 січня 2020 р. при відправці моніторингової інформації

Як видно з результатів проведених експериментів, використання протоколу UDP як основного (поверх якого здійснюється тунелювання протоколу UDP за допомогою технології OpenVPN) можна вважати ефективним для прийому моніторингової інформації (UDP-трафіку) по VPN-тунелю. Однак при передачі команд керування для блоку керування радіоетелескопом, представленого у вигляді низькоінтенсивного нееластичного трафіку, доцільно використовувати протокол TCP поверх протоколу UDP. Це пояснюється тим, що існує більша ймовірність втрати пакетів, через відсутність механізмів адаптації трафіку до поточного стану нестійкого каналу зв'язку в РАО, а саме механізму регулювання розміру вікна, – протокол UDP показує більш низькі результати, ніж TCP. Механізм повторних передач для моніторингової інформації, що реалізується з використанням протоколу TCP (еластичний трафік) дозволяє компенсувати втрачені пакети за рахунок повторних команд, що відправляються з програмного буфера керуючої програми віддаленої обчислювальної станції.

6. АПРОБАЦІЯ РЕЗУЛЬТАТІВ

Основні результати наукового дослідження були представлені на науково-практичній конференції 2019 IEEE International Conference on Advanced Trends in Information Theory ATIT, яка проводилася у Київському національному університеті імені Тараса Шевченка 18-20 грудня 2019 року за підтримки IEEE Ukraine Section та IEEE Ukraine Section Information Theory Society Chapter [12].

Результати наукової роботи впроваджені в постійну експлуатацію на радіотелескопі ГУРТ Радіоастрономічної обсерваторії імені академіка С.Я. Брауде Радіоастрономічного інститут Національної академії наук України та отримано відповідний акт впровадження від 02 грудня 2019 року (додаток А).

Також за результатами обговорення на засіданні Постійно діючої комісії з навчально-методичної роботи та атестації аспірантів кафедри Електронних обчислювальних машин факультету Комп'ютерної інженерії та управління ХНУРЕ (Протокол № 4 від 20 грудня 2019 року) – отримано відповідний акт про використання результатів наукової роботи у навчальному процесі (акт від 28 грудня 2019 року) (додаток Б).

ВИСНОВКИ

В роботі сформульована та успішно вирішена науково-прикладна задача розробки технології віддаленого керування науковими інструментами на платформі оверлейних мереж. Зокрема:

- сформульована задача з формалізацією необхідних технічних вимог до розроблюваної оверлейной комп'ютерної мережі;
- розроблено метод організації оверлейної мережі, заснований на використанні вкладених (багатошарових) VPN-тунелів;
- проведені експерименти з дослідження ефективності використання різних транспортних мережних протоколів в VPN-тунелях;
- запропонована технологія впроваджена в постійну експлуатацію для віддаленого керування радіотелескопом ГУРТ в Радіоастрономічному інституті НАН України.

Необхідно відзначити, що об'єднання VPN-тунелів в каскадні схеми випадковим чином є не ефективним для побудови великих оверлейних мережних інфраструктур для організації віддаленого керування. Незважаючи на те, що пропускна здатність залежить від топології комп’ютерної мережі, необхідно проводити аналіз розподілу VPN-тунелів для підвищення надійності процесу передачі даних. Таким чином, можна зробити висновок, що аналіз загальної пропускної здатності VPN-тунелів багато в чому залежить від правильної організації маршрутизації даних на VPN-серверах і правилами налаштування шлюзів для уникнення можливих неефективних маршрутів передачі даних.

У якості подальшої дослідницької роботи, яка має відображення при підготовці атестаційної роботи бакалавра, пропонується розглянути ефективність застосування анонімних оверлейних мереж для проміжного транспорту даних між VPN-серверами.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Значення науки у незалежній Україні [Електронний ресурс] // Веб-сайт Освіта.ua, дата публікації: 19.01.2009. Режим доступу: http://osvita.ua/vnz/reports/ history/4119.

2. Редько О.І. Аналіз комп'ютерних технологій і прогнози їхнього розвитку в майбутньому / О.І. Редько, Р.Г. Редько, Н.Т. Зубовецька, О.М. Пагуба // Наукові нотатки. – 2015. – №. 52. – С. 60-62.

3. Січкаренко К.О. Результати інтеграції українських наукових установ в європейський науковий простір // Економічний вісник Запорізької державної інженерної академії. – 2017. – №. 3. – С. 38-43.

4. Толубко В.Б. Впровадження LTE-серйозний поштовх до розвитку Інтернет речей / В.Б. Толубко, Л.Н. Беркман, О.А. Хахлюк // Наукові записки Українського науково-дослідного інституту зв'язку. – 2017. – №. 3. – С. 5-10.

5. Могилова А.Ю. Ретроспективний аналіз розвитку ринку інтернет-провайдингу в Україні / А.Ю. Могилова, А.Г. Девлетшаєва // Економіка і суспільство. – 2018. – №. 16. – С. 187-191.

6. Wu P. Analysis of the WireGuard protocol // Master's Thesis. – Eindhoven University of Technology, Department of Mathematics and Computer Science. – June 17, 2019. – 88 p.

7. Drugarin C.V.A., Draghici S., Raduca E. Team Viewer Technology for Remote Control of a Computer // Analele Universitatii' Eftimie Murgu'. – 2016. – Vol. 23. – №. 1. – Pp. 61-66.

8. Pascual R. P. Implementación de una red privada virtual de software libre en una empresa. – Universitat Oberta de Catalonya. – 2019. – P. 12.

9. Barabanova I.A., Kravets O.J., Tkalich S.A., Mutin D.I. Analysis of the intermediate layer work in the three-tier architecture "client-server" of automation engineering problems // IOP Conference Series: Materials Science and Engineering. – IOP Publishing, 2019. – Vol. 537. – №. 3. – P. 032011.

10. Jyothi K.K., Reddy B. Study on virtual private network (VPN), VPN's protocols and security //International Journal of Scientific Research in Computer Science, Engineering and Information Technology. – 2018. – Vol. 3. – №. 5. – Pp. 919-932.

11. Кулаков А. Ю. Способ повышения эффективности GRID систем на базе виртуальных сетей VPN // Вісник Національного технічного університету України Київський політехнічний інститут. Сер.: Інформатика, управління та обчислювальна техніка. – 2007. – №. 47. – С. 282-288.

12. Tkachov V., Bondarenko M., Ulyanov O., Reznichenko O. Overlay Network Infrastructure for Remote Control of Radio Astronomy Observatory // 2019 IEEE International Conference on Advanced Trends in Information Theory ATIT. – 18-20.12.2019 – Kyiv, Ukraine. – 5 p.

13. Термін «Інформаційна технологія». Закон України від 04.02.1998 № 74/98-ВР «Про Національну програму інформатизації» [Електронний ресурс] // Веб-сайт Законодавство України, дата публікації: 04.02.1998. Режим доступу: https://zakon.rada.gov.ua/laws/term/11482:11723/sp?sp=s6:max15.

14. Konovalenko A. The modern radio astronomy network in Ukraine: UTR-2, URAN and GURT / A. Konovalenko, L. Sodin, V. Zakharenko, P. Zarka, O. Ulyanov, M. Sidorchuk, …, G. Mann // Experimental Astronomy. – 2016. – Vol. 42. – №. 1. – Pp. 11-48.

15. Юзьків І. Аналіз використання пакетів TCP і UDP в мережах VPN // Матеріали науково-технічної конференції „Інформаційні моделі, системи та технології ". – 2018. – С. 90-90.

16. Шейда В. В. Использование протоколов TCP и UDP для защищенной передачи информации по SSL-VPN-туннелям // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2010. – №. 1-2 (21).

АНОТАЦІЯ НАУКОВОЇ РОБОТИ
ПІД ШИФРОМ «Віддалений доступ»

Актуальність роботи – необхідність організації віддаленого керування науковими інструментами (приладами) виникає при проведенні спільних наукових досліджень.

Завдання наукової роботи – розробка технології віддаленого керування науковими інструментами на платформі оверлейних комп'ютерних мереж.

Об'єкт дослідження – комп'ютерна мережа наукового інструменту (обсерваторії, станції тощо).

Предмет дослідження – метод організації вкладених VPN-тунелів між вузлами комп'ютерної мережі

Мета роботи – розробка технології віддаленого керування науковими інструментами на базі оверлейних комп'ютерних мереж, яка включає в себе побудову віртуальних та вкладених багатошарових тунелів.

Метод дослідження – активні експерименти при побудові оверлейної мережі.

Загальна характеристика роботи: 30 с., 5 рис., 2 табл., 16 джерел, 2 додатки.

КОМП'ЮТЕРНА МЕРЕЖА, ВІДДАЛЕНИЙ ДОСТУП, ОВЕРЛЕЙНА МЕРЕЖА, VPN