

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
РАДІОЕЛЕКТРОНІКИ

ІСААМ СААД

УДК 621.391

**МОДЕЛІ І МЕТОДИ АНАЛІЗУ ТА ВЕРИФІКАЦІЇ ПРОТОКОЛІВ
УПРАВЛІННЯ У ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖАХ, ЩО
БАЗУЮТЬСЯ НА АЛГЕБРИ КОМУТАЦІЙНИХ РОЗПОДІЛЕНИХ РЕСУРСІВ
ТА ГРАФАХ ДОСЯЖНОСТІ**

Спеціальність 05.12.02 – телекомунікаційні системи та мережі

АВТОРЕФЕРАТ

дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2016

Дисертацією є рукопис.

Робота виконана в Харківському національному університеті радіоелектроніки Міністерства освіти і науки України.

Науковий керівник: доктор технічних наук, доцент
ДУРАВКІН Євген Володимирович,
Харківський національний університет
радіоелектроніки,
професор кафедри телекомунікаційних систем.

Офіційні опоненти: доктор технічних наук, доцент
ГАРКУША Сергій Володимирович,
Полтавський університет економіки і торгівлі
Укоопспілки,
доцент кафедри інформаційної діяльності в
економічних системах;

кандидат технічних наук, доцент
КИРИК Мар'ян Іванович,
Національний університет «Львівська політехні-
ка», МОН України
доцент кафедри телекомунікацій

Захист відбудеться «26» жовтня 2016 року о 15 годині на засіданні спеціалізованої вченої ради Д 64.052.09 в Харківському національному університеті радіоелектроніки за адресою: Україна, 61166, м. Харків, пр. Науки, 14.

З дисертацією можна ознайомитися у бібліотеці Харківського національного університету радіоелектроніки за адресою: 61166, м. Харків, пр. Науки, 14.

Автореферат розісланий «20» вересня 2016 року.

Учений секретар
спеціалізованої вченої ради
кандидат технічних наук, доцент
Ткачова

О.Б.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Одним із важливих напрямків розвитку телекомунікаційних систем та мереж є забезпечення та підтримка високого рівня якості сервісів, що надаються. Однак стрімке зростання об'ємів та розширення функціональних можливостей сервісів призводить до ускладнення мережевих протоколів управління та передачі, а, відповідно, й до підвищення рівня складності мережевого обладнання.

Концепція програмно-конфігурованих мереж (Software-Defined Networking, SDN) дозволяє підвищити ефективність функціонування телекомунікаційної мережі за рахунок відокремлення функцій управління від функцій передачі даних. Основним протоколом, що забезпечує обмін управляючими повідомленнями та відповідає за організацію взаємодії між рівнем управління та рівнем передачі даних є OpenFlow. Від коректності функціонування протоколу OpenFlow залежить коректність функціонування всієї мережі в цілому.

Однією з проблем розвитку концепції SDN є те, що протокол OpenFlow не має остаточної кінцевої реалізації та вимоги щодо його функціонування постійно змінюються. Ряд компаній, які розробляють мережеве обладнання (Cisco, HP, Juniper, Mikrotik та ряд інші), використовують власні модифікації протоколу. Така ситуація призводить до виникнення несумісності та відсутності підтримки необхідних функціональних вимог. Відсутність єдиної уніфікованої специфікації також є причиною ряду помилок, що виникають у процесі проектування SDN рішень.

Сучасні підходи, що застосовуються при розробці протоколів управління мережевими ресурсами, не дозволяють забезпечити належну якість протоколу OpenFlow. Так, наприклад, обчислювальна потужність методів формалізації вимог специфікації, що набули широкого значення під час розробки традиційних телекомунікаційних протоколів недостатня для формалізації складних процесів взаємодії типу «комутатор-контролер-комутатор».

Застосування математичних методів та моделей у процесі розробки протоколу OpenFlow дозволяє поліпшити процеси формалізації вимог до протоколу, аналізу та оцінки коректності поведінки, оптимізувати процес перевірки відповідності реалізації протоколу його специфікації. Слід зазначити, що під час використання традиційних підходів верифікації виникає ряд труднощів, пов'язаних з недосконалістю сучасних методів: залежно від обраного методу (тестування або формальна верифікація) можливе виявлення обмеженої кількості помилок або, навпаки, виникнення ефекту «комбінаторного вибуху» простору досліджуваних станів.

Таким чином виникає задача розробки нових та вдосконалення існуючих методів підтримки процесів розробки протоколів управління у програм-

но-конфігурованих мережах, що забезпечать скорочення часу їх розробки та підвищення ефективності функціонування мережі.

Завданнями розвитку концепції SDN, а саме дослідженням та удосконаленням методів розробки та впровадження протоколу OpenFlow, займаються передові IT-компанії, такі як Cisco, HP, IBM, Juniper та ряд видатних академічних кіл - ONF, IRTF, IETF, ETSI, SDNRG. Методам дослідження та розробки протоколу OpenFlow, зокрема, моделям та методам аналізу коректності поведінки та перевірки відповідності реалізації протоколу специфікації, присвячений ряд робіт закордонних дослідників Макломса Б., Канін М., Менезес П., Томаса А., Шервуда Р. Питанням аналізу, розробки та адаптації OpenFlow рішень також присвячено ряд робіт російських та українських вчених - Захарова В. А., Смілянського Р. Л., Кучерявого А.Є., Чемерецкого Є.В. та ін.

Грунтуючись на результатах аналізу попередніх досліджень встановлено, що одним з найбільш перспективних напрямків вирішення вказаних недоліків є розвиток математичних моделей та методів, які дозволять підвищити ефективність процесу розробки та впровадження за рахунок внесення однозначності та строгих формалізмів на різних етапах розробки.

Отже дисертаційна робота, що присвячена вирішенню задачі розробки та вдосконаленню методів аналізу та верифікації протоколів управління у програмно - конфігурованих мережах, що базуються на алгебрі комутаційних розподілених ресурсів та графах досяжності є актуальною.

Зв'язок роботи з науковими програмами, планами, темами. Завдання дисертаційного дослідження тісно пов'язані з положеннями «Концепції Національної програми інформатизації», «Концепції розвитку електронного урядування в Україні», «Концепції створення та функціонування інформаційної системи електронної взаємодії державних електронних інформаційних ресурсів». Матеріали дисертаційної роботи реалізовані в ході виконання науково-дослідної роботи № 299-1 «Методи проектування телекомунікаційних мереж NGN та управління їх мережевими ресурсами» (№ ДР 0115U002432).

Запропоновані моделі та методи аналізу та верифікації протоколу OpenFlow використані у навчальному процесі кафедри телекомунікаційних систем Харківського національного університету радіоелектроніки (ХНУРЕ), зокрема в дисципліні «Перспективні телекомунікаційні технології» та «Інформаційні системи та Інтернет». Використання результатів дисертаційної роботи підтверджено відповідними актами впровадження.

Метою роботи є підвищення якості управління в програмно-конфігурованих мережах за рахунок вдосконалення процесів розробки та впровадження протоколів управління.

Для досягнення цієї мети в роботі поставлено та вирішено наступні **задачі**:

- розробка методу формалізації вимог специфікації протоколу OpenFlow, що представлені на підмножині природної мови, за допомогою алгебри комунікаційних розподілених ресурсів;
- розробка методів пошуку та усунення протиріч між вимогами в рамках специфікації протоколу OpenFlow;
- розробка методу синтезу моделі E-мережі реалізації протоколу на основі формалізмів алгебри комунікаційних розподілених ресурсів;
- розробка методу побудови дерева досяжності для моделі реалізації протоколу, представленої на базі апарату E-мережі;
- розробка алгоритму послідовного розбору та перевірки відповідності дерева досяжності моделей реалізації та специфікації протоколу;
- розробка методу побудови контрприкладу, що дозволяє виявити причини виникнення помилок та невідповідностей у реалізації протоколу, а також вказати шляхи їх усунення.

Об'єкт дослідження: процес розробки, аналізу та верифікації протоколу OpenFlow.

Предмет дослідження: математичні моделі і методи аналізу та верифікації протоколу OpenFlow, що базуються на алгебрі комутаційних розподілених ресурсів та графах досяжності.

Методи дослідження. Підчас розв'язання поставлених задач було використано наступні методи: апарат алгебри комунікаційних розподілених ресурсів, зокрема, використання його семантичних та синтаксичних складових підчас розробки методу формалізації специфікації; апарат E-мереж та математичні методи аналізу функціональних і нефункціональних властивостей протоколу підчас вирішення задачі перевірки коректності протоколу OpenFlow; формальні методи верифікації, такі як символний підхід та Model Checking підчас розробки методу перевірки відповідності моделі реалізації протоколу вимогам специфікації.

Наукова новизна отриманих результатів. В ході розв'язання поставлених задач були отримані наступні нові наукові результати:

1. Отримав подальший розвиток математичний апарат алгебри комунікаційних розподілених ресурсів як інструмент формалізації вимог специфікації протоколів управління, зокрема протоколу OpenFlow. Новизна запропонованого підходу полягає в тому, що оператори алгебри комунікаційних розподілених ресурсів використано як засіб формалізації процесів та подій, що дозволяє враховувати як структурні, так і кількісні характеристики. Вперше запропоновано метод перевірки та пошуку протиріч в рамках специфікації

протоколу OpenFlow шляхом послідовного порівняння формалізмів вимог специфікації.

2. Отримав подальший розвиток апарат E-мереж як засіб моделювання поведінки протоколу OpenFlow. Вперше впроваджено застосування управляючих переходів для моделювання функціональних властивостей протоколу та використання кількісних значень атрибутів переходів таких, як «порогові значення» у процесі функціонування, що дозволило розширити множину моделюючих станів, та підвищити ступінь деталізації.

3 Отримали подальший розвиток методи аналізу алгебраїчних властивостей E-мереж, новизна полягає в розробці алгоритму побудови дерева досяжності моделі E-мережі, що дозволило виявляти можливі цикли та підцикли у процесі функціонування протоколів управління.

4 Вперше розроблено метод верифікації протоколу OpenFlow, який дозволяє виконати як часткову перевірку на основі шаблонів, так і повну перевірку, уникаючи при цьому ефекту «комбінаторного вибуху» простору досліджуваних станів та запропоновано алгоритм побудови контрприкладу на основі аналізу дерева досяжності.

Обґрунтованість і достовірність отриманих в роботі нових наукових результатів забезпечувалась та підтверджувалась коректним використанням ключових положень відомого та апробованого математичного апарату - логіках нижчого та вищого порядку, теорії управління багаторівневими системами, теорії графів та поширеними підходами до процесу верифікації.

Наукове значення. Запропоновані у дисертаційному дослідженні математичні моделі та методи аналізу та верифікації дозволяють вдосконалити процеси розробки, впровадження та експлуатації програмних складових та мережевого обладнання, що функціонує на базі протоколу OpenFlow, так і SDN мережі в цілому.

Результати дисертаційної роботи можуть бути рекомендовані при проектуванні та вдосконаленні конвергентних телекомунікаційних систем, а запропоновані моделі та методи можуть бути використані як науково-методична база для подальших досліджень функціонування протоколу OpenFlow та інших, що функціонують у програмно-конфігурованих мережах, та створення нових засобів підтримки процесу розробки.

Практична значимість результатів досліджень полягає в тому, що запропоновані математичні моделі і методи можуть бути використані під час розробки, підтримки, проектування та впровадження різноманітних телекомунікаційних систем та мереж, що базуються на хмарному підході та використанні концепції програмно-конфігурованих мереж, зокрема OpenFlow протоколу. Запропонована методика була використана для перевірки коректності поведінки протоколу OpenFlow під час балансування мережевої загруз-

ки та пошуку помилок при сумісному функціонуванні різних версій протоколу OpenFlow (v 1.0.0 та v 1.3.0) у межах спільного фрагменту мережі; пошуку протиріч між реалізаціями протоколу OFDP та верифікації поведінки протоколу OpenFlow на стадії встановлення з'єднання та збору інформації про зміну топології мережі. Результати дисертації використані в ході виконання науково-дослідної роботи № 299-1 «Методи проектування телекомунікаційних мереж NGN та управління їх мережевими ресурсами» (№ ДР 0115U002432), в якій дисертант виступав співвиконавцем.

Особистий внесок здобувача. Всі основні наукові результати, висвітлені в дисертаційній роботі, здобувач отримав самостійно. Крім того, в роботі [1] автором розроблені формалізми, що визначають правила композиції та узгодження комплексних Web-сервісів, які дозволяють об'єднати елементи розподіленої інфокомунікаційної мережі в єдину систему. У роботі [2] автором запропоновано метод верифікації розподілених систем, що базується на модельному підході та дозволяє враховувати асинхронну природу комплексних сервісів. У роботі [3] автором проведено аналіз розвитку концепції SDN та сформовано ряд основних завдань дослідження. У роботі [4] автором запропоновано метод аналізу протоколу OpenFlow, в основі якого лежить модельний підхід та застосування апарату E-мереж, також наведено метод аналізу таких властивостей моделі реалізації протоколу, як досяжність, обмеженість, безпечність та жвавність. У роботі [5] автором запропоновано застосування математичного апарату алгебри комунікаційних розподілених ресурсів як одного з методів формалізації специфікації, що дозволяє повноцінно формалізувати причинно-наслідкові зв'язки між подіями і процесами, що формують поведінку протоколу. У роботі [6] автором запропонована методика аналізу і верифікації яку засновано на модельному підході і перевірці відповідності послідовності зміни станів протоколу OpenFlow. У роботі [7] запропоновано метрику оцінки масштабованості рівня управління, а також приведена оцінка зміни коефіцієнта масштабованості трьох основних структур рівня управління Software-Defined Networking: централізованої, децентралізованої, ієрархічної. У роботі [8] автором запропоновано новий метод аналізу функціональних та нефункціональних вимог до реалізації протоколу OpenFlow. Модифікований метод базується на побудові моделі E-мережі протоколу та подальшому аналізі її алгебраїчних властивостей за допомогою дерева досяжності. Запропонований підхід дозволяє враховувати кількість запусків переходів E-мережі, виникнення зациклювань та тупікових вершин-позицій.

Апробація основних положень дисертаційної роботи була проведена у ході чотирьох конференцій та одного форуму, а саме у Другій Міжнародній

науково-технічній конференції «Проблемы инфокоммуникаций. Наука и технологии (PICS&T)» (2014 р., м. Харків, ХНУРЕ), у другій Всеукраїнській науково-технічній конференції «Проблеми розвитку глобальної системи зв'язку, навігації, спостереження та організації повітряного руху CNS/ATM» (2014р., м. Київ, Інститут аеронавігації НАУ), у Першій Міжнародній науково-практичній конференції «Проблеми телекомунікацій» (2014 р., м. Харків, ХНУРЕ), у Першій Міжнародній науково-технічній конференції «Проблеми електромагнітної сумісності перспективних безпроводних мереж зв'язи ЕМС –2015» (2014 р., м. Харків, ХНУРЕ) та у 19-му Міжнародному молодіжному форумі «Радиоэлектроника и молодежь в XXI веке» (2015 р., м. Харків, ХНУРЕ).

Публікації. Основні результати дисертаційної роботи опубліковані в восьми наукових статтях. З них шість наукових статей опубліковані в наукових фахових виданнях України [1, 3, 4, 5, 6, 7] та дві статті у зарубіжних фахових виданнях [2, 8]. Матеріали дисертаційних досліджень тезисно опубліковані в 5 збірниках науково-технічних конференцій, в тому числі й публікації, проіндексовані і наукових базах IEEEExplore.

Структура та обсяг дисертації. Дисертація складається зі вступу та чотирьох розділів. Загальний обсяг роботи становить 209 сторінок, в тому числі 173 сторінок основного тексту, 49 рисунків та 6 таблиць на 19 сторінках. Список використаних джерел містить 157 найменувань, викладених на 17 сторінках.

ЗМІСТ РОБОТИ

У **вступі** розкрито стан проблем, що досліджуються, обґрунтовано актуальність теми дисертаційної роботи, визначено мету досліджень та ряд науково-практичних задач, що повинні бути вирішені для досягнення поставленої мети. Наведено наукову новизну та практичне значення отриманих результатів. Надано дані щодо апробації отриманих результатів та публікації автора за темою дисертації.

У **першому розділі** проведено аналіз архітектури та протоколів управління у SDN. У результаті проведених досліджень було встановлено, що існуючі проблеми, які виникають під час функціонування SDN у більшості випадків пов'язані з наявністю декількох діючих версій специфікацій, які містять внутрішні відмінності та протиріччя.

У якості моделі життєвого циклу протоколу запропоновано використовувати спіральну модель. Її основними перевагами є можливість враховувати динамічні зміни вимог до реалізації та постійне оновлення вимог специфікації, а також одночасне урахування та аналіз декількох версій протоколу OpenFlow. Зазначено, що на кожному етапі життєвого циклу спіральної мо-

делі впроваджуються підетапи перевірки результатів та можливість повернення на попередній етап.

Так, на етапі формування вимог специфікації запропоновано застосовувати алгебру комутаційних розподілених ресурсів (algebra of communication shared resources, ACSR). Аналіз показав, що апарат ACSR дозволяє найбільш повно описати хронологію виникнення подій з урахуванням часу та тривалості їх виконання.

Аналіз реалізації протоколу запропоновано проводити на моделі протоколу, що побудована за допомогою апарату E-мереж. Вибір апарату E-мереж обумовлений високим рівнем універсальності та наявністю керуючих переходів. При використанні такого підходу можлива побудова моделі протоколу з різним ступенем деталізації. Наявність керуючих переходів дозволяє також враховувати безліч особливостей OpenFlow протоколу.

На етапі тестування запропоновано проводити формальну верифікацію. Застосування модельного підходу (Model Checking) дозволяє охопити можливу кінцеву множину інваріантів поведінки протоколу та виконати поступову перевірку їх відповідності вимогам специфікації. Виявлення розбіжностей між реалізацією протоколу і вимогами його специфікації та пошук шляхів їх усунення базується на побудові контрприкладу.

Застосування класичного підходу Model Checking підчас верифікації протоколу OpenFlow у більшості випадків є неможливим через виникнення ефекту «комбінаторного вибуху» простору досліджуваних станів. На підставі чого прийнято рішення про необхідність розробки модифікованого методу верифікації на базі підходу Model Checking, що дозволяє усунути ефект «комбінаторного вибуху».

У **другому розділі** у рамках вирішення задачі формалізації вимог специфікації протоколу OpenFlow запропоновано використання апарату алгебри комунікаційних розподілених ресурсів. Для перевірки збереження функціональних та нефункціональних властивостей у реалізації протоколу запропоновано проводити аналіз основних алгоритмічних властивостей E-мережі.

Відповідно до рекомендацій ETSI та ITU-T на етапах аналізу вимог та формування специфікації основні функціональні властивості протоколів наводяться за допомогою однієї з підмножин природної мови або за допомогою SDL чи UML діаграм. Використання таких підходів при розробці протоколу OpenFlow має ряд обмежень: двоякість термінів та понять, відсутність можливості урахування тривалості процесів, природи (синхронні чи асинхронні) та пріоритетів їх виникнення, призводить до помилкового розуміння вимог специфікації на початкових стадіях та подальшої реалізації помилкових тверджень. Доповнення або оновлення вимог специфікації в ряді випадків викликає виникнення протиріч між ними, наприклад, застосування різних ко-

манд для виконання однієї дії, різна послідовність та методика обробки повідомлень протоколу OpenFlow.

Наведений у першому розділі аналіз методів формалізації вимог специфікації показав, що апарат ACSR в повній мірі дозволяє формально описати умови виконання процесів, їх пріоритет та часові залежності завдяки розширеній множині темпоральних операторів, відповідній семантиці та правилам виводу формалізмів.

На основі базових правил ACSR складено типові шаблони поведінки протоколу OpenFlow, які є істинними у процесі всього життєвого циклу протоколу. З метою побудови семантично вірних формалізмів специфікації за допомогою ACSR сформульовано послідовність кроків, що дозволяє однозначно формалізувати вимоги специфікації. Основними з них є:

1 Формування множини елементарних тверджень (символів алфавіту), що мають ключове значення при функціонуванні протоколу OpenFlow.

2 Формується множина процесів, що обумовлюють переходи з одного стану в інший.

3 На базі отриманої множини елементарних тверджень формуються зв'язки між ними, що утворюють певний стан. Визначається тип стану: початковий, проміжний або заключний.

4 Формуються трійки типу «стан протоколу-процес-стан протоколу»:

4.1 Встановлюється хронологічна послідовність між процесами.

4.2 Встановлюється пріоритет виконання кожного процесу.

4.3 Визначаються логічні зв'язки між кожною сформованою трійкою.

4.4 Визначається наявність паралельного виконання декількох трійок «стан протоколу-процес-стан протоколу».

На базі сформованих за допомогою апарату алгебри комутаційних розподілених ресурсів тверджень також розроблено методи перевірки та виявлення суперечностей у вимогах специфікації. Перший метод базується на алгоритмі поступового порівняння формалізмів специфікації, що містять однакові елементи та перевірки логіки їх виконання. Другий метод ґрунтується на оцінці досяжності графу станів специфікації протоколу. Вершинами графу є події, що мають місце під час функціонування протоколу, дуги відображають виконання процесів.

Зазначено, що ефективність функціонування протоколу OpenFlow значною мірою залежить від його програмної реалізації, а також особливостей реалізації мережевої операційної системи контролера та правил обробки пакетів на комутаторах.

Перевірку функціональних та нефункціональних вимог запропоновано проводити на моделі реалізації протоколу. Як апарат моделювання запропоновано використовувати E-мережі та проводити аналіз таких алгоритмічних

властивостей, як обмеженість, досяжності, жвавості, збереження та безпечність.

Розроблено метод синтезу моделі Е-мережі на базі ACSR формалізмів, що відповідають вимогам специфікації. Також розроблено метод однозначного перетворення процесів та станів формалізмів ACSR в переходи і позиції Е-мережі.

В якості методу аналізу розглянуто застосування матричних рівнянь, формальних граматики та дерева досяжності. Вдосконалено метод побудови дерева досяжності, що дозволяє враховувати типи переходів Е-мережі. Дерево досяжності задано наступною множиною:

$$G(D) = \langle P, H, \gamma \rangle, \quad (1)$$

де $P = \{p_1, p_2, \dots, p_n\}$ – множина вершин-позицій дерева, що відповідає множині досяжних розміток Е-мережі реалізації протоколу $D(M_f)$; $H = \{e_{ij}\} (\forall p_j, p_j \in V)$ – множина переходів, активність яких призводить до досягнення певної розмітки M' , $M' \in M_f$; $\gamma: f(H \rightarrow P)$ – функція спрацьовування переходів.

Розроблений метод побудови модифікованого дерева досяжності включає декілька додаткових етапів та складається з наступної послідовності дій:

1 Визначення початкового маркування (розмітки) M_0 Е-мережі та формування множини потенційно активних переходів.

2 Визначення множини потенційно досяжних вершин. У випадку, якщо потенційно досяжні вершини існують:

2.1 Для кожної вершини визначається її тип: термінальна, дублююча або гранична.

Нехай існують потенційно досяжні вершини x та y :

- якщо маркування вершини x (розмітка M_x) та вершини y (розмітка M_y) співпадають, то вершина y визначається як дублююча.

- якщо маркування вершини x та y не співпадають ($M_x \neq M_y$) та не існує активних переходів з вершини y , то вершина y визначається як термінальна, а її маркування M_y – заключним.

– якщо маркування вершини x та y не співпадають $M_x \neq M_y$ та існують активні переходи з вершини y у будь-яку іншу вершину моделі реалізації протоколу, то вершина y вважається граничною, а вершина x помічається як внутрішня.

2.2 Визначення множини активних переходів, що призводять до зміни маркування мережі.

Встановлюється відповідність вершини x певній позиції Е-мережі p_x (M_x) та вершини y – позиції p_y (M_y) та значення переходу, який переводить маркування M_x у маркування M_y .

3 Виконання кроків 1-2 здійснюються до тих пір, поки існують досяжні маркування. Дерево досяжності вважається сформованим після того, як отримано усі термінальні, дублюючі або граничні вершини.

4 Формування множин $\{M_f'(p_i)\}$, $\{M_f'(h_{i-1})\}$, що визначають маркування задіяні у процесі переміщення мітки від кореня дерева до певної термінальної вершині з множини M_f .

4.1 Встановлюється кількість запусків проходів (проходження мітки через кожну досяжну вершину: внутрішню, дублюючу або граничну) при побудові повного дерева досяжності.

а) якщо на шляху від кореневої вершини до заключного станом існує вершина i , така що $M_i \rightarrow M_f$, $M_i < \gamma(M_f, h_{f-1})$ ($M_i)_\omega < \gamma(M_f, h_{f-1})_\omega$, то $(M_i)_\omega = \omega$ або $(M_i)_\omega = (0, 0, \dots, \omega, \dots, 0)$

б) якщо $(M_f)_\omega = \omega$, то $(M_z)_\omega = \omega$, де ω – значення лічильника керуючого переходу.

4.2 Визначення першого моменту появи символу ω , що відповідає мульти запускам переходу. Встановлюється тип активного переходу. У цьому випадку, якщо перехід відноситься до управляючих M_X, M_Y та містить атрибут (лічильник, то кожен раз при запуску переходу значення лічильника збільшується на одиницю. Далі, на основі отриманих результатів, визначається вектор розміток. Під вектором розміток розуміється упорядкована множина всіх доступних вершин-позицій, що задіяні у процесі досяжності заключної вершини. Для кожного вектору розмітки формується індивідуальна гілка дерева досяжності.

Нехай $M_0 = (\underbrace{1, 0, 0, 0, \dots, 0}_k)$ – початкова розмітка Е-мережі або корінь дерева досяжності, k – кількість потенційно досяжних вершин. Наявність «1» маркуванні вершини визначає номер задіяної позиції Е-мережі. Так як справедливі наступні твердження $M_0 = (\underbrace{p_1, 0, 0, 0, \dots, 0}_k)$, $M_1 = (\underbrace{0, p_1, 0, 0, \dots, 0}_k), \dots$
 $M_k = (\underbrace{0, 0, 0, 0, \dots, p_k}_k)$, то вектор розміток може бути заданий як $\overline{M_{0k}} = (\underbrace{p_1, p_2, p_1, \dots, p_k}_k)$. Результуючий вектор розміток для відповідного кінцевого маркування складається із сукупності усіх векторів розмітки. Результуючий вектор розмітки запропоновано формалізувати наступним чином:

$$\overline{\sum M_{ok}} = \left(\underbrace{\sum_1^n p_1, \sum_1^m p_2, \sum_1^l p_i, \dots, \sum_1^j p_k}_{k} \right) = \left(\underbrace{p^1_1, p^m_2, p^l_i, \dots, p^j_k}_k \right), \quad (2)$$

де n, m, l, j – кількісне значення проходжень міткою зазначених вершин-позиції.

Загальний вигляд дерева досяжності, що включає множину усіх можливих гілок, запропоновано нотувати наступним чином:

$$\begin{aligned} T(M_f) &= \overline{\sum M_{ok}} \cup \overline{\sum M_{on}} \cup \overline{\sum M_{op}} = \\ &= \left(\underbrace{\sum_1^n p_1, \sum_1^m p_2, \sum_1^l p_i, \dots, \sum_1^j p_k}_{k} \right) \cup \left(\underbrace{\sum_1^n p_1, \sum_1^m p_2, \sum_1^l p_i, \dots, \sum_1^j p_n}_n \right) \cup \left(\underbrace{\sum_1^n p_1, \sum_1^m p_2, \sum_1^l p_i, \dots, \sum_1^j p_p}_p \right). \end{aligned} \quad (3)$$

Структурна схема алгоритму побудови модифікованого дерева досяжності наведена на рис. 1.

Запропоновано метод синтезу Е-мережі за формалізмами ACSR, що відповідають вимогам специфікації. Підґрунтям запропонованого методу є метод трансляції алгебри процесів у кінцеві автомати та табличний метод перетворення формул темпоральної логіки у граф станів. Синтез Е-мережі за формалізмами алгебри комунікаційних розподілених ресурсів включає наступну послідовність дій:

1 Формування множини вершин-позицій, що відповідає множині *Act* вимог специфікації. У цьому випадку кожна позиція Е-мережі характеризується множиною *State* та включає наступні параметри:

State = [*ID*: *StateID*; *CURRENT*: *current state definition*; *INCOMING*: *previous transmission*; *OUTCOMING*: *next transmission*],

де *ID* – унікальний ідентифікатор вершини-позиції; *CURRENT* – поточний символ алфавіту, що належить алфавіту алгебри комунікаційних розподілених ресурсів та відповідає поточній вершині-позиції; *INCOMING* – множина вхідних переходів; *GOING* – множина вихідних переходів.

2 Формування множини вершин-переходів, що відповідає множині $M(X, p)$ вимог специфікації. У цьому випадку кожен перехід Е-мережі визначається множиною *Transition* та включає наступні параметри:

Transition = [*ID*: *Transition ID*, *CURRENT*: *current Transition definition*; *AT*: *atribute*, *INCOMING*: *previous state*, *OUTCOMING*: *next state*],

де *ID* – унікальний ідентифікатор вершини-переходу; *CURRENT* – поточний символ алфавіту, що належить до ACSR та відповідає даному перехо-

ду; *INCOMING* – множина вхідних позицій; *GOING* – множина вихідних позицій, *AT* – предикат переходу. Встановлення відносин інцидентності.

Застосування Е-мереж, як одного з методів моделювання протоколу OpenFlow та запропонованого методу побудови дерева досяжності моделі протоколу як одного з методів аналізу дозволило розв’язати такі задачі, як аналіз досяжності необхідного стану або дії, що відповідають функціональним та не функціональним вимогам специфікації.

У **третьому розділі** розроблено метод верифікації протоколу OpenFlow. У процесі розробки методу верифікації до уваги прийнято основні відмінні особливості етапів розробки OpenFlow, такі як наявність декількох прототипів та мінливість вимог щодо реалізації. Запропонований метод базується на основі результатів попередніх етапів: Е-мережі моделі реалізації протоколу та формалізованому дереві досяжності, що відповідає наведеній реалізації протоколу. Відмінною рисою розробленого методу є розширення множини вхідних даних до процесу верифікації та використання набору шаблонів.

У процесі розробки методу верифікації розглянуто ряд ситуацій, що потребують виконання перевірки відповідності моделі реалізації вимогам специфікації. Такими ситуаціями є часткова перевірка відповідності реалізації протоколу вимогам специфікації, часткова перевірка відповідності реалізації протоколу множині шаблонів та повна перевірка відповідності реалізації протоколу вимогам специфікації. На основі розглянутих ситуацій виділено декілька варіантів верифікації реалізації протоколу:

- Часткова перевірка відповідності реалізації протоколу вимогам специфікації або перевірка відповідності основних властивостей. Процес верифікації запропоновано формалізувати наступним чином:

$$\begin{aligned} ((f_i, S_{iOF}, P_i)_{\text{мод}} \equiv (f_i, S_{iOF}, P_i)_{\text{вимога}}) \\ \{(f, S_{OF}, P)_{\text{вимога}}\} \in (f, S_{OF}, P)_{\text{мод}} \end{aligned} \quad (4)$$

де P – множина процесів, що зазначені у специфікації протоколу та потребують перевірки, P_i відповідає взаємодії можливих станів протоколу OpenFlow S_{OF} , $f: P \rightarrow S_{OF}$ – функція залежності, що відображає основні причини –наслідкові зв’язки між процесами та подіями, (f, S_{OF}, P) – узагальнена динамічна система, $(f, S_{OF}, P)_{\text{мод}}$ – система, що відповідає реалізації OpenFlow, $(f, S_{OF}, P)_{\text{вимога}}$ – система, що відповідає властивостям або вимогам специфікації протоколу OpenFlow.

- Часткова перевірка відповідності реалізації протоколу його специфікації, що ґрунтується на перевірці відповідності шаблонам поведінки

різних версій протоколу. Процес верифікації запропоновано формалізувати наступним чином:

$$\begin{aligned} ((f_i, S_{iOF}, P_i)_{\text{мод}} \equiv (f_i, S_{iOF}, P_i)_{\text{шаблон}}) \\ \{(f, S_{SDN}, P)_{\text{шаблон}}\} \in (f, S_{SDN}, P)_{\text{мод}} \end{aligned} \quad (5)$$

де $(f_i, S_{iOF}, P_i)_{\text{шаблон}}$ – прототип реалізації, що включає обов'язковий уніфікований набір вимог та тверджень.

- повна перевірка відповідності реалізації протоколу вимогам специфікації. Такий тип перевірки формально визначається наступним чином:

$$\begin{aligned} ((f, S_{OF}, P)_{\text{мод}} \equiv (f, S_{OF}, P_i)_{\text{спец}}) \\ \{(f, S_{OF}, P)_{\text{мод}}\} \in (f, S_{OF}, P)_{\text{спец}} \end{aligned} \quad (6)$$

де $(f_i, S_{iOF}, P_i)_{\text{спец}}$ – модель специфікації, що залежить від поточної версії специфікації протоколу.

Структурна схема процесу верифікації наведена на рис. 1.

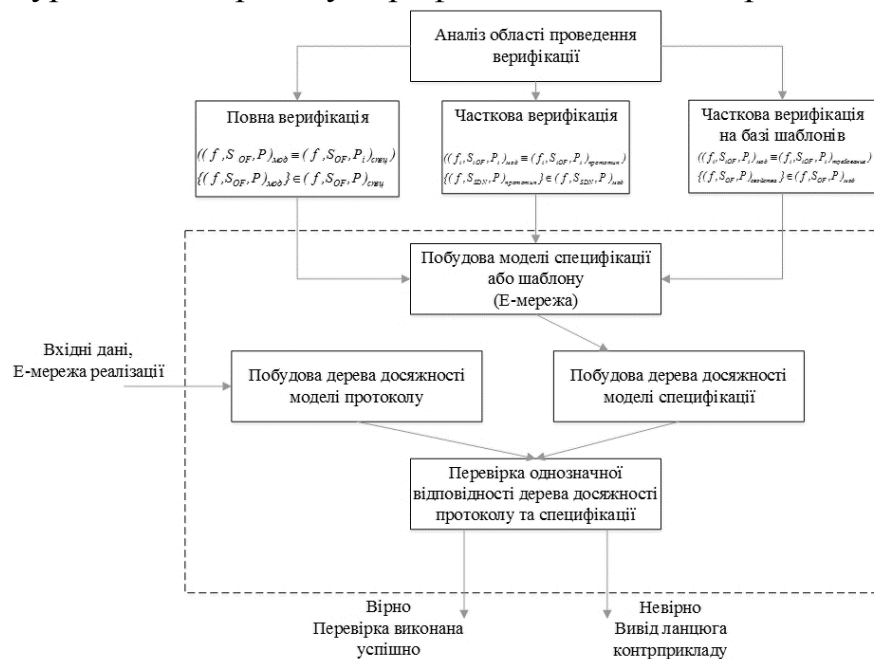


Рис. 1. Процес перевірки відповідності моделі реалізації протоколу вимогам специфікації

З метою підвищення ефективності процесу верифікації та зменшення ефекту «комбінаторного вибуху» простору досліджуваних станів, запропоновано наступний метод, що базується на класичному підході Model Checking:

1 Етап моделювання.

1.1 Побудова моделі реалізації протоколу, якщо вона не зазначена у вхідних даних.

1.2 Побудова моделі специфікації протоколу.

2 Етап верифікації.

2.1 Визначення області верифікації.

2.2 Процес верифікації.

Знаходження відповідності між вершинами дерева досяжності моделі реалізації та моделі специфікації протоколу відбувається на основі вирішення наступної системи рівнянь:

$$R_i(s_{C_i}, s_{M_i}) = \begin{cases} M(s_{M_i}) \in M(s_{C_i}), \\ s_{C_i}, True / s_{C_i} \equiv s_{M_i}, \\ \delta(s_{C_{i-1}}, s_{C_i}) \equiv \delta(s_{M_{i-1}}, s_{M_i}), \\ \text{and} \\ 0, False / s_{C_i} \neq s_{M_i}, \\ \delta(s_{C_{i-1}}, s_{C_i}) \neq \delta(s_{M_{i-1}}, s_{M_i}), \end{cases} \quad (7)$$

де S_M – множина усіх можливих вершин моделі реалізації протоколу, S_C – множина усіх можливих вершин моделі специфікації протоколу, s_{M_i} – поточна вершина моделі реалізації, s_{C_i} – поточна вершина моделі специфікації; $s_{C_{i-1}}$ та $s_{C_{i+1}}$ – попередня вершина та вершина, що слідує за вершиною s_{C_i} , $s_{M_{i-1}}$ у моделі специфікації та $s_{M_{i+1}}$ – попередня вершина-позиція та вершина, що слідує за вершиною s_{M_i} у моделі реалізації.

3. Аналіз результатів процесу верифікації та формування контрприкладу.

Якщо під час виконання процесу верифікації помилки знайдено, то відбувається побудова контрприкладу. При побудові контрприкладу формується множина станів протоколу $M(S')$, де $S' \in F \cup \neg F$. Основною вимогою формування контрприкладу є досяжність одного з термінальних станів. Побудова контрприкладу у випадку виникнення циклів базується на алгоритмах «подвійного обходу» та пошуку у глибину. У якості апробації запропонованого методу наведено верифікацію алгоритму виявлення у фрагменті мережі каналів зв'язку з недостатньою пропускнуною спроможністю. Процес верифікації було виконано двома методами: методом символної перевірки та розробленим методом. Результати, отримані в процесі верифікації дають змогу зробити висновок, що розроблений метод дозволяє виявити таку ж саму множину помилок, як і добре символний метод SPIN. Але, на відміну від символного підходу, запропонований метод верифікації дозволяє виявити та сформулювати послідовність дій та станів, що призводять до виникнення помилок.

У **четвертому розділі** на сформувано узагальнену методику аналізу та верифікації протоколу OpenFlow. Узагальнена методика передбачає використання цілей та результатів кожного попереднього етапу процесу розробки,

внесення рекомендацій щодо засобів досягнення поставлених цілей. Кожний етап запропонованої загальної методики може бути використаний як окремий модульний підхід, що робить її застосування універсальним та передбачає подальше використання розроблених моделей та методів як до протоколів, що розробляються, так і вже існують. Структурна схема узагальненої методики наведена на рис. 2.

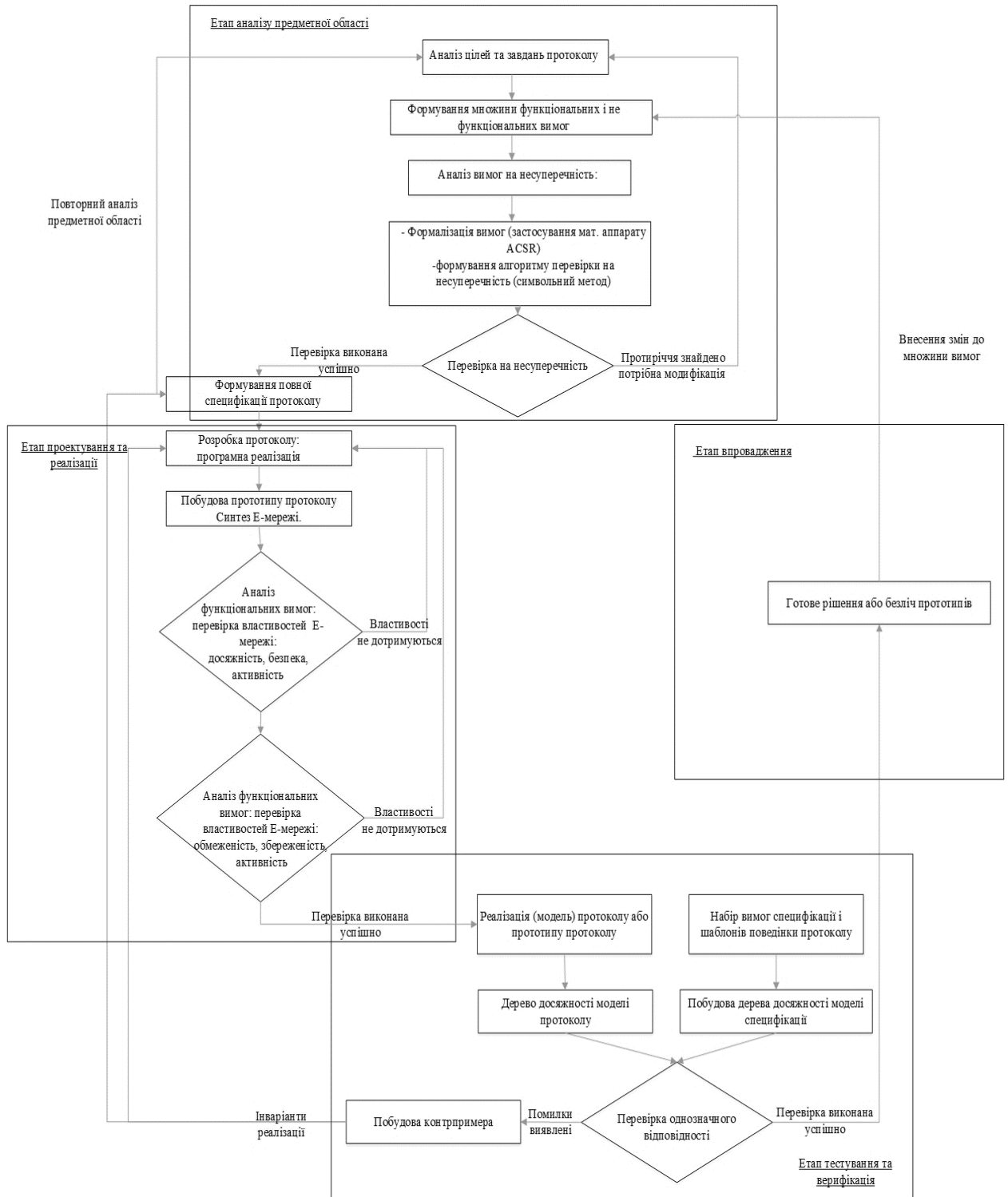


Рис.2. Структурна схема узагальненої методики аналізу та верифікації протоколу OpenFlow

Для оцінки ефективності розробленої методики аналізу та верифікації проведено експериментальні дослідження. У якості основного критерію ефективності обрано трудомісткість етапів процесу розробки - кількість людино-годин, що витрачено на кожному етапі розробки.

Отримані дані дозволили встановити, що використання розробленої методики аналізу та верифікації дозволяє підвищити ефективність розробки телекомунікаційних протоколів на 20%. Зазначено, що кількість часу, витраченого у процесі впровадження та верифікації була суттєво знижена (на етапі проектування виграш склав 10%, на етапі реалізації - 7%), це пов'язано з наявністю додаткових методів перевірки вимог специфікації.

В рамках оцінки ефективності і коректності розробленого методу верифікації досліджено кілька ситуацій функціонування протоколу OpenFlow. Імітаційне моделювання було проведено за допомогою програмного продукту Mininet.

Порівняльні дані, що отримано в результаті проведення експерименту наведено у таблиці 1.

Таблиця 1

Значення часу верифікації та кількість виявлених помилок

Вимога, що потребує перевірки/критерії оцінювання	Розроблений метод		Метод SPIN	
	Час верифікації (мс)	Кількість виявлених помилок	Час верифікації (мс)	Кількість виявлених помилок
Збір інформації про топології мережі за допомогою протоколу OFDP	0,040	2	0,037	1
Обміну інформацією між OpenFlow комутаторами	0,585	3	0,501	2
Перевірка доступності мережевих ресурсів	0,130	4	0,129	4

На основі наведених результатів дослідження зроблено висновок, що розроблений метод верифікації в деяких випадках дозволяє виявити більшу кількість помилок у реалізації протоколу OpenFlow, ніж широко поширені методи верифікації телекомунікаційних систем, наприклад SPIN. Час, витрачений на верифікацію за допомогою розробленого методів в ряді випадків менше часу, витраченого при застосуванні SPIN. Для наведеного прикладу виграш в разі використання пропонованого методу верифікації становить 22%.

ВИСНОВКИ ПО РОБОТІ

В роботі розв'язана *актуальна науково-прикладна задача*, що полягає у розробці нових та вдосконалення існуючих методів підтримки процесів розробки протоколів управління у програмно-конфігурованих мережах, що забезпечують скорочення часу розробки протоколів та дозволять підвищити ефективність функціонування мережі за рахунок впровадження математичних методів аналізу та верифікації на базі апарату E-мереж, алгебри комунікаційних розподілених ресурсів та підходу Model Checking.

За підсумками вирішення задачі можна зробити наступні висновки:

1. Аналіз поточного стану та перспектив розвитку телекомунікаційних систем та мереж показав, що ключове значення у процесі впровадження нових сервісів, мають складність обладнання, що використовується, та кінцева вартість впровадження. Все частіше на сучасні мережеве обладнання, а саме комутатори та маршрутизатори, накладається ряд додаткових функцій, що призводить до їх ускладненого функціонування та негативно впливає на якість наданих послуг. Одним з методів удосконалення процесів надання послуг є розділення функцій управління та функцій передачі даних, що відносяться до різних типів мережевого обладнання. Саме на цьому принципі відокремлення рівня управління від рівня передачі даних базується концепція SDN.

2. Аналіз основних складових компонентів архітектури та протоколів, що забезпечують взаємодію між рівнями та елементами SDN, показав, що існуючі проблеми функціонування SDN мереж пов'язані з відсутністю чітко визначених вимог та стандартизованих специфікацій протоколів, наявністю декількох версій специфікацій та їх внутрішніми відмінностями; використання різних мережевих операційних систем на рівні управління також впливає на показники якості обслуговування. Виявлення та усунення протиріч у вимогах специфікацій, функціональних розбіжностей та помилок, пов'язаних з програмною реалізацією протоколу OpenFlow та SDN контролеру дозволить гармонізувати процес функціонування мережі та підвищити загальні показники QoS.

3. Встановлено, що значна кількість помилок виникає підчас формування вимог та розробки специфікації протоколу OpenFlow. Запропоновано використовувати спіральну модель життєвого циклу, що дозволяє враховувати динамічну модернізацію та оновлення вимог до функціонування протоколу. Впровадження стадії аналізу результатів, що отримано на кожному етапі дозволяє виявити більшу кількість помилок та усунути можливість їх виникнення на подальших етапах, що суттєво впливає на вартість розробки та впровадження протоколів управління.

4. У якості методу формалізації вимог специфікації запропоновано використовувати алгебри комунікаційних розподілених ресурсів. Важливою відмінністю апарату алгебри комунікаційних розподілених ресурсів від існуючих математичних методів формалізації специфікації є можливість нотування паралельних та асинхронних процесів, відображення пріоритетів процесів та формалізація часових залежностей між ними. На основі базових правил алгебри комунікаційних розподілених ресурсів сформовано шаблони поведінки, які є істинними в процесі всього життєвого циклу протоколу.

С метою виявлення протиріч у вимогах специфікації протоколу OpenFlow розроблено метод, що базується на послідовному співставленні однакових символів формалізмів ACSR і встановлені їх синтаксичної та семантичної несуперечності. Використання даного методу дозволило підвищити ефективність аналізу вимог специфікації, а також скоротити ймовірність виникнення помилок на подальших етапах розробки.

5. З метою усунення помилок на етапі реалізації запропоновано проводити аналіз функціональних та нефункціональних властивостей реалізації протоколу за допомогою модельного підходу. У якості математичного апарату моделювання запропоновано використовувати апарат E-мереж, як один з найбільш адекватних методів моделювання протоколу OpenFlow. Розроблено метод синтезу E-мереж на основі формалізмів алгебри комунікаційних розподілених ресурсів, що відображають вимоги специфікації. Запропоновано проводити аналіз таких алгоритмічних властивостей, як: обмеженість, активність, досяжність та безпечність.

6. В якості методу аналізу алгоритмічних властивостей E-мереж запропоновано використання дерева досяжності. Запропоновано модифікацію методу дерева досяжності, що дозволяє відобразити поведінку протоколу під час досягнення бажаних заключних станів, та, відповідно, дозволить проаналізувати коректність поведінки, а також збереження основних властивостей під час функціонування протоколу.

7. Заключним етапом розробки протоколу OpenFlow у відповідності до спіральної моделі життєвого циклу є етап тестування та верифікації. Аналіз основних методів, які застосовуються під час верифікації складних телекомунікаційних систем, показав, що їх використання у процесі пошуку відповідності реалізації протоколу OpenFlow вимогам специфікації, неможливе за рахунок наступних недоліків: недостатня виразність логічних формалізмів, необмежений час проведення верифікації, виявлення тільки шаблонного набору помилок, ефект «комбінаторного вибуху» простору станів та інші. В рамках вирішення задачі перевірки відповідності реалізації протоколу OpenFlow вимогам специфікації, запропоновано новий метод верифікації, що базується на класичному підході методу Model Checking.

8. У рамках оцінки ефективності запропонованого методу проведено експеримент: верифікацію фрагменту мережі двома методами – розробленим методом та методом SPIN. У результаті порівняння отриманих у ході виконання експерименту даних встановлено, що запропонований метод дозволяє виявити більшу кількість помилок. Виграш від використання розробленого методу склав 22%.

9. На основі розроблених моделей та методів аналізу та верифікації сформовано узагальнену методичку аналізу та верифікації протоколу OpenFlow. Етапи загальної методички відповідають етапам та принципам функціонування спіральної моделі життєвого циклу. Рекомендації та доповнення, внесені на кожному етапі, дозволили підвищити ефективність процесу розробки. Апробацію розробленої методички було проведено під час виконання проекту «Flow Balance». Дані, отримані в ході дослідження, дозволили встановити, що використання запропонованої методички дозволяє підвищити ефективність процесу розробки до 17%.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Иссам С. Метод верификации комплексных Web –сервисов / С. Иссам, Я. А. Раед, О.Б. Ткачева // Проблемы телекоммуникаций. – 2014. – №1 (13). – С. 63 – 73. : http://pt.journal.kh.ua/2014/1/1/141_tkacheva_soap.pdf
2. Issam Saad Verification method of complex Web –services / S. Issam, O. Tkachova A. Raed // Journal of Future Internet, 2014, 1(1): 1–15 [электронная версия] режим доступа http://www.pakinsight.com/pdf_files/JFI_2014_1%281%29_1_15.pdf
3. Иссам Саад. Архитектура SDN. Анализ основных проблем на пути развития / Е.Б. Ткачева, Е.В. Дуравкин, Иссам Саад // Системы обработки информации: зб. наук. праць Харківського університету Повітряних Сил, 2015. – Вип. 3(128). – С.92 –98.
4. Иссам Саад. Применение аппарата E –сетей для решения задач анализа и верификации программно –конфигурируемых сетей / Е.Б. Ткачева, Иссам Саад, Мохаммед Джамал Салим // Вісник НТУ «ХПІ». Серія: Інформатика і моделювання, 2015. – Вип. 32 (1141). – С.148–159.
5. Иссам Саад. Применение ASCR для верификации протоколов управления Software –Defined Network / Е.Б. Ткачева, Иссам Саад, Мохаммед Джамал Салим // Радиотехника: Всеукр. межвед. научн. техн. сб., 2015. – Вип. 180. – С.48 –56.
6. Issam S. Mathematical models for analysis Software-Defined Network/ S. Issam, M. J. Salim, Tkachova O. // International Journal "Information Technologies & Knowledge", 2015 – Vol. 9 (2) – Pp.111–123.

7. Иссам Саад. Анализ и оценка масштабируемости уровня управления сетей, построенных на основе концепции SDN / Иссам Саад, О.Б. Ткачева, Мохаммед Джамал Салим // Системи обробки інформації збірник наукових праць. – Х.:Харківський університет Повітряних Сил імені І. Кожедуба, 2015 – Вип. 9(134), – 2015. – С.133–137.
8. Isaam Saad. A Method of Behavioral Analysis of OpenFlow Protocol / Isaam Saad, Tkachova O. // Scholars Journal of Engineering and Technology, 2016. – Vol. 3(128). – С.92 –98.
9. Isaam Saad. Method for OpenFlow protocol verification / Isaam Saad, O.B. Tkachova, // Second International IEEE Conference «Problems of Infocommunications. Science and Technology» PICS&T–2015, 13–15 October 2015: proc. of the conf. – Kharkiv, Ukraine, 2015. – Pp. 139 –140.
10. Isaam Saad, Tkachova O. Methods for specification and verification of complex Web-services / Infocommunications Science and Technology. First International Scientific–Practical Conference «Problems of Infocommunications. Science and Technology» PICS&T –2014, 14–17 Oct. 2014: proc. of the conf. – Kharkiv, Ukraine, 2014. – Pp. 139 –140.
11. Иссам Саад. Методы формального анализа программно конфигурируемых сетей / Иссам Саад, Ткачева Е. Б., Фаиз Мобхот // Всеукраїнська науково –технічна конференція «Проблеми розвитку глобальної системи зв'язку, навігації, спостереження та організації повітряного руху CNS/АТМ» – Київ, Інститут аеронавігації НАУ. –2014. – с.62
12. Иссам Саад. Оценка масштабируемости уровня управления в программно–конфигурируемых сетях / Иссам Саад, Ткачева Е. Б. // Друк Материалы 1–ой Международной научно–технической конференции «Проблемы электромагнитной совместимости перспективных беспроводных сетей связи ЭМС – 2015, 27 мая 2015 – Харьков: ХНУРЭ, 2015. – Pp. 137 –140.
13. Иссам Саад. Метод анализа свойств программно – конфигурируемых сетей на базе аппарата E–сетей / Материалы 19–го международного молодежного форума «Радиоэлектроника и молодежь в XXI веке». – Часть 4. – Харьков: ХНУРЭ, 2015. – с.58.

АНОТАЦІЯ

Исаам Саад. Моделі і методи аналізу та верифікації протоколів управління у програмно-конфігурованих мережах, що базуються на алгебрі комутативних розподілених ресурсів та графах досяжності. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.12.02 – Телекомунікаційні системи та мережі. – Харківський національний університет радіоелектроніки, Харків, 2016.

Дисертаційну роботу присвячено розв'язанню задачі розробки нових та вдосконалення існуючих методів та моделей підтримки процесів розробки протоколів управління у програмно-конфігурованих мережах, що дозволяють забезпечити скорочення часу розробки протоколів та підвищити ефективність функціонування мережі. У якості формалізації вимог специфікації протоколів управління запропоновано використання математичного апарату алгебри розподілених комутаційних ресурсів, що дозволяє однозначно інтерпретувати твердження специфікації. Застосування алгебри розподілених комутаційних ресурсів у якості інструменту побудови специфікації дозволяє виявити протиріччя між твердженнями специфікації.

Задачу аналізу реалізації протоколу запропоновано звести до розв'язання задач перевірки відповідності таких функціональних та нефункціональних властивостей OpenFlow протоколу, як обмеженість, жвавість, досяжність, безпечність, покриваємість. З метою автоматизації процесу побудови моделі протоколу розроблений метод синтезу моделі E-мережі за ACSR формалізмами тверджень специфікації.

Запропоновано новий метод верифікації протоколів управління, в основу якого покладено класичний підхід «перевірки на моделях». Процес верифікації у випадку використання запропонованого методу базується на послідовній перевірці відповідності гілок дерева досяжності E-мережі моделі реалізації та специфікації протоколу OpenFlow. На основі часткових розроблених методів сформовано комплексну методику аналізу та верифікації протоколів управління у програмно-конфігурованих мережах.

Ключові слова: протокол OpenFlow, дерево досяжності, алгебра розподілених комутаційних ресурсів, верифікація, функціональні властивості протоколу.

АННОТАЦІЯ

Исаам Саад. Модели и методы анализа и верификации протоколов управления в программно-конфигурированных сетях базирующиеся на алгебре коммуникационных распределенных ресурсов и графах достижимости. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.12.02 – телекоммуникационные системы и сети. Харьковский национальный университет радиоэлектроники, Харьков, 2016.

Диссертационная работа посвящена решению актуальной задачи, заключающейся в совершенствовании процессов разработки и внедрения протоколов управления в программно-конфигурируемых сетях, в частности протокола OpenFlow. С целью решения поставленной задачи разработан ряд методов, позволяющих сократить вероятность возникновения ошибок и разно-

гласий на начальных стадиях процесса разработки, а также уменьшить их влияние на последующие этапы.

В качестве инструмента формализации требований спецификации протоколов управления предложено применение математического аппарата алгебры распределенных коммутационных ресурсов, который позволяет однозначно интерпретировать утверждения спецификации, учитывать приоритеты выполнения процессов и причинно-следственные связи между ними. На основе формализмов алгебры распределенных коммутационных ресурсов разработан метод проверки противоречий, базирующийся на поэлементном сопоставлении формализмов утверждений, содержащих одинаковые символы алфавита темпоральной логики, и анализе взаимоисключения ветвей достижимости графа состояний.

Задача анализа сохранения требуемых функциональных и нефункциональных свойств в реализации протокола сведена к решению задачи анализа основных алгоритмических свойств модели E-сети таких, как ограниченность, живость, достижимость, безопасность и сохраняемость. С целью автоматизации процесса построения модели протокола разработан метод синтеза модели E-сети по формализмам ACSR, отображающим требования спецификации: предложен метод однозначного преобразования процессов и состояний протокола OpenFlow в вершины-переходы и вершины-позиции модели E-сети. Разработан модифицированный метод построения дерева достижимости, который позволяет нивелировать возникновение символа ω путем учета количественного значения прохождения меткой вершин-позиций в процессе функционирования. Такой подход позволяет формализовать поведение протокола в процессе достижения заключительных состояний, и, соответственно, проанализировать сохранение требуемых свойств.

Предложен новый подход к верификации протоколов управления, в основу которого положен классический метод «проверки на моделях». Процесс верификации в данном случае базируется на последовательной проверке соответствия ветвей дерева достижимости E-сети модели реализации и ветвей дерева достижимости спецификации протокола OpenFlow. Разработан алгоритм формирования контрпримера, который обеспечивает вывод и позволяет локализовать последовательность состояний модели реализации протокола, приводящих к возникновению ошибок. Сформировано несколько сценариев процесса верификации: частичная верификация на основе шаблонов и полная верификация реализации протокола. Применение такого подхода позволяет уменьшить вероятность возникновения эффекта «комбинаторного взрыва» пространства состояний.

На основе частных моделей и методов сформирована комплексная методика анализа и верификации протоколов управления в программно-

конфигурируемых сетях. Полученные в диссертационном исследовании результаты нашли практическое применение при выполнении НИР и в учебном процессе.

Ключевые слова: протокол OpenFlow, дерево достижимости, алгебра распределенных коммуникационных ресурсов, верификация, функциональные свойства протокола.

ABSTRACT

Issam Saad. The models and methods for analysis and verification control protocols in Software-Defined Networks based on apparatus of algebra communication shared resources and reachability graphs. – Manuscript.

Dissertation work submitted in satisfaction of the requirements for the degree of Doctor of Philosophy in technical sciences within specialty 05.12.02 – telecommunication systems and network. – Kharkiv National University of Radio Electronics, Kharkiv, 2016.

The dissertation work is devoted to solving the problem of developing new and improving existing methods and models that support development processes of control protocols in Software-Defined Networks for future reduction time of protocols development and increase the efficiency of network functionality. The mathematical apparatus of algebra communication shared resources is proposed to use as a method, which allow to uniquely interpreting the statement of specifications and give ability to formalize the priority, parallel execution and causal relationships between processes that take place in specification's statements. Methods of contradiction detect in OpenFlow protocol specification are also suggested.

A method of analysis functional and non-functional requirements of OpenFlow protocol realization is proposed. The modified reachability tree for compliance and behaviour analysis of model of OpenFlow protocol is proposed in the paper. The proposed method bases on modelling approach and give ability analyse the protocol functionality on earlier stages of realization.

A new method of control protocol verification that based on the classic "model checking" approach is proposed. The process of verification includes consistent verification of reachability tree branches that belong to model of protocol implementation and model of specification respectively. The complex methodology of analysis and verification is developed. The proposed complex approach is based on particular developed methods and models.

Keywords: OpenFlow protocol, reachability tree, algebra of communication shared resources, verification, functional properties of the protocol.