Національний технічний університет України

**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Інститут телекомунікаційних систем**

Кафедра інформаційно-телекомунікаційних мереж

«На правах рукопису»

УДК 004.021

«До захисту допущено»

Завідувач кафедри

_____ Лариса ГЛОБА

«___»_____2020 р.

Магістерська дисертація

**на здобуття ступеня магістра
за освітньо-професійною програмою «Інформаційно-комунікаційні технології»
зі спеціальності 172 «Телекомунікації та радіотехніка»
на тему: «Метод управління безпекою інформаційних потоків мережі IoT за допомогою SDN»**

Виконав:
студент ІІ курсу, групи ТІ-91мп
Марчук Олександр Олегович _____

Керівник:
Професор кафедри ІТМ ІТС, д.т.н, с.н.с
Скулиш Марія Анатоліївна _____

Рецензент:
Професор кафедри ІТМ ІТС, д.т.н, проф.
Лисенко Олександр Іванович _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2020

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем

Кафедра Інформаційно-телекомунікаційних мереж

Рівень вищої освіти – другий (магістерський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інформаційно-комунікаційні технології»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Лариса ГЛОБА

«___»_____2020 р.

ЗАВДАННЯ

на магістерську дисертацію студенту

Марчуку Олександру Олеговичу

1. Тема дисертації «Метод управління безпекою інформаційних потоків мережі IoT за допомогою SDN», науковий керівник дисертації професор кафедри інформаційно-телекомунікаційних мереж ІТС Скулиш Марія Анатоліївна, д.т.н., затверджені наказом по університету від «03» листопада 2020 р. № 3208-с
2. Термін подання студентом дисертації 10.12.2020 р.

3. Об’єкт дослідження: пристрої і технології організації зв'язку в мережі Інтернету речей

4. Предмет дослідження: Моделі передачі даних і методи забезпечення функціонування пристроїв Інтернету речей в умовах впливу небезпек

5. Перелік завдань, які потрібно розробити:
    1. здійснити літературний огляд за темою дослідження;
    2. розкрити поняття інформаційних потоків;
    3. описати сутність, поняття, генезис інтернету речей;
    4. навести проблематику дослідження та постановку завдань;

5. провести проектування програмно-конфігурованої мережі на базі IoT;

6. запропонувати модель управління безпекою інформаційних потоків мережі IoT;

7. навести алгоритм управління безпекою інформаційних потоків мережі IoT за допомогою SDN;

8. розкрити методологію визначення ефективності управління безпекою інформаційних потоків мережі IoT за допомогою SDN;

9. описати ефективність управління безпекою інформаційних потоків мережі IoT за допомогою SDN.

6. Орієнтовний перелік ілюстративного матеріалу:

1. Тема, мета, актуальність, задачі дослідження.
2. Аналіз існуючих підходів щодо управління безпекою інформаційних потоків мережі IoT за допомогою SDN.
3. Удосконалений спосіб управління безпекою інформаційних потоків мережі IoT за допомогою SDN.
4. Результати експерименту та імітаційного моделювання роботи мережі IoT за допомогою SDN.
5. Загальні висновки.

7. Орієнтовний перелік публікацій

8. Дата видачі завдання 01.09.2019 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Вибір та обґрунтування напрямку дослідження	01.09.2019 – 30.09.2019	виконано
2	Дослідження використання технології SDN	01.10.2019 – 30.11.2019	виконано
3	Порівняльна оцінка існуючих методів проектування програмно-конфігурованої мережі на базі IoT	01.12.2019 – 28.02.2020	виконано
4	Оцінка аналіз існуючих методів проектування програмно-конфігурованої мережі на базі IoT	01.03.2020 – 15.04.2020	виконано
5	Опис та постановка задачі для розгортання мережі IoT за допомогою SDN	16.04.2020 – 31.05.2020	виконано
6	Апробація теоретичних результатів дослідження	1.06.2020 – 30.06.2020	виконано

7	Підготовка середовища, планування та проведення експерименту з метою отримання вихідних даних	1.07.2020 - 30.09.2020	виконано
8	Аналіз отриманих результатів та формування практичних рекомендацій	01.10.2020 - 30.11.2020	виконано
9	Підготовка звітної документації	01.12.2020 - 21.12.2020	виконано

Студент Олександр МАРЧУК

Науковий керівник дисертації Марія СКУЛИШ

РЕФЕРАТ

Робота містить 104 сторінки, 26 рисунків та 19 таблиць. Було використано 70 джерел.

Актуальність: Підвищення якості функціонування мереж зв'язку за рахунок поліпшення надійності є складною науково-технічною та економічною проблемою. Це обумовлено тим що до мереж з новими технологіями, таким як програмно-конфігуровані мережі (SDN) в даний час висувають високі вимоги по надійності (відмовостійкості) в тому числі до характеристик відновлення мережі після відмови. При розробці заходів, що підвищують надійність доцільна постановка задачі максимально можливого підвищення якості функціонування мережі при мінімальному часу відновлення зв'язку.

Високий рівень відмовостійкості мережі забезпечується за рахунок швидкого виявлення пошкоджень і усунення їх наслідків за короткий час. Існуючі методи забезпечення надійності в мережах SDN можна поділити на два самостійних класи: захисне перемикання (резервування) і відновлення (перемаршрутизація). Звідси випливає що для системного підходу до дослідження методів забезпечення надійності SDN доцільно використовувати засоби математичного моделювання.

Дослідження механізмів забезпечення надійності SDN розглядається в ряді робіт, як вітчизняних, так і зарубіжних. Однак в даних роботах не проводиться порівняльний аналіз використання механізмів забезпечення відмовостійкості, а також комбінації цих механізмів. Так само в ряді робіт не враховуються економічні показники використання даних механізмів.

Мета роботи: підвищити відмовостійкість при DoS-атаці системи Інтернету речей з використанням концепції SDN за рахунок премаршутизації та резервування комунікаційних ресурсів, що дозволить зменшити час до виявлення відмови методами швидкого відновлення, зменшиння відсотка навантаженості.

Задачі дослідження:

1. Проаналізувати існуючі підходи щодо управління безпекою інформаційних потоків мережі IoT за допомогою SDN .
2. Запропонувати модель управління безпекою інформаційних потоків мережі IoT при DoS-атаці, яка дозволить зменшити як ймовірність відмови, так і вплив відмови ;
3. Вдосконалити процедуру керування безпекою інформаційних потоків мережі IoT яка враховує можливості організації потоків в програмно-керованих мережах (SDN);
4. Розробити удосконалений метод управління безпекою інформаційних потоків мережі IoT з використанням концепції SDN та резервування контролера, що дозволить отримати надійну мережу, не враховуючи збільшення часу до виявлення відмови при роботі методів швидкого відновлення.
5. Розробка імітаційної моделі в середовищі MiniNet, планування та проведення експерименту з метою перевірки теоритичних положень та доведення їх ефективності.
6. Розробка стартап проекту для системи безпеки IoT.

Об’єкт дослідження: пристрої і технології організації програмно-керованого зв'язку в мережі Інтернету речей.

Предмет дослідження: моделі та методи управління безпекою інформаційних потоків мережі IoT за допомогою SDN

Методи дослідження: Проведені дослідження базуються на теорії ймовірностей, математичній статистиці, теорії телекомунікацій методах моделювання. Моделювання фрагмента мережі IP проведено на основі пакета MiniNet.

Наукова новизна: Запропоновано удосконалений метод управління безпекою інформаційних потоків мережі IoT з використанням концепції SDN, який дозволяє підвищити відмовостійкість при DoS-атаці системи Інтернету речей, зменшити час до виявлення відмови методами швидкого відновлення,

зменшити відсотка завантаженості мережі, за рахунок премаршутизації та резервування комунікаційних ресурсів.

Практична новизна: Пропонована модель PFI скорочує час на встановлення шляху, знижує час обробки контролера і зменшує трафік каналу управління при DoS-атаці на мережу шляхом використання методів резервування та відновлення зв’язку, також взаємодіє з протоколами безпеки, основним з них є OpenFlow

Ключові слова: SDN, програмно-конфігурована мережа, віртуалізація мережевих функцій, IoT, IP.

ABSTRACT

The work contains 104 pages, 26 figures and 19 tables. 70 sources were used.

Relevance: Improving the quality of communication networks by improving reliability is a complex scientific, technical and economic problem. This is due to the fact that networks with new technologies, such as software-configured networks (SDN) currently have high requirements for reliability (fault tolerance), including the characteristics of network recovery after failure. When developing measures to increase reliability, it is advisable to set the task of maximizing the quality of network operation with a minimum connection recovery time.

The high level of fault tolerance of the network is provided due to fast detection of damages and elimination of their consequences in a short time. Existing methods of ensuring reliability in SDN networks can be divided into two separate classes: protective switching (redundancy) and recovery (rerouting). It follows that for a systematic approach to the study of methods to ensure the reliability of SDN, it is advisable to use mathematical modeling.

The study of the mechanisms of ensuring the reliability of SDN is considered in a number of works, both domestic and foreign. However, these works do not provide a comparative analysis of the use of mechanisms to ensure fault tolerance, as well as a combination of these mechanisms. Similarly, a number of works do not take into account the economic indicators of the use of these mechanisms.

Purpose: to develop a method of managing the security of information flows of the IoT network using the concept of SDN and controller redundancy, which will provide a reliable network, without taking into account the increase in time to detect failure of rapid recovery methods.

Research objectives:

1. to propose a model of security management of information flows of the IoT network;

2. provide an algorithm for managing the security of information flows of the IoT network using SDN;

3. to reveal the methodology for determining the effectiveness of security management of information flows of the IoT network using SDN;

4. to develop an improved method of managing the security of information flows of the IoT network using the concept of SDN and controller redundancy, which will allow to obtain a reliable network, without taking into account the increase in time to detect failure of fast recovery methods.

Object of research: devices and technologies of communication organization in the Internet of Things.

Subject of research: data transmission models and methods of ensuring the functioning of the Internet of Things in the face of hazards.

Research methods: The research is based on probability theory, mathematical statistics, modeling methods and field experiments. The simulation of a fragment of the IP network was performed on the basis of a simulation package.

Scientific novelty: An improved method of managing the security of information flows of the IoT network using the concept of SDN and controller redundancy has been proposed, which will allow to obtain a reliable network, without taking into account the increase in time to detect failure of fast recovery methods.

Practical novelty: The obtained results can be implemented in a real enterprise in order to improve the quality of security management of information flows of the IoT network using SDN.

Keywords: SDN, software-configured network, virtualization of network functions, IoT, IP.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

SDN	software-defined networking
NFV	Network Functions Virtualization
ПКМ	програмно-керована мережа
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
OVS	Open vSwitch
FL	Floodlight
FV	FlowVisor

ВСТУП

Концепція Інтернету речей (IoT - Internet of Things) [32, 33] принципово змінила уявлення наукового та інженерного співтовариства про мережі зв'язку, як в кількісному, так і в якісному відношенні. Основним змістом і призначенням Інтернету речей (IP) є надання інформації користувачам про фізичні або віртуальні об'єкти із заданою якістю обслуговування [4]. Для реалізації цієї вимоги необхідна інтеграція великого обсягу інформації про об'єкти та їх ідентифікації в мережі. Таке визначення речей призвело до різкого збільшення самої мережі, а наслідком цього і числа користувачів в мережах Інтернету речей. За оцінками, представленими в [7], до 2025 року в мережі IP прогнозується зберігання інформації про 25 мільярдів речей. В даний час мережі IP є одними з найбільш затребуваних і зручних для збору і передачі великих обсягів інформації. У зв'язку з цим вивченню мережі IP присвячено багато робіт вітчизняних і зарубіжних вчених А. Е. Кучерявого, Е. А. Кучерявого, А. В. Рослякова, Р. В. Киричка, А. П. Пшеничникова, Е. В. Турута, Д. А. Молчанова, В. А. Мочалова, П. А. Абакумова, А. В. Прокоп'єва, W. Heinzelman, O. Yonis, D. Kim, K. Lindsey, A. Salim.

Поряд з усіма перевагами мережі IP, зважаючи на свою глобальність і складність, стають все більш уразливими до дії дестабілізуючих чинників різної природи.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ УПРАВЛІННЯ БЕЗПЕКОЮ ІНФОРМАЦІЙНИХ ПОТОКІВ МЕРЕЖІ ІОТ ЗА ДОПОМОГОЮ SDN

1.1 Літературний огляд за темою дослідження

Можливості платформи Internet of Things (IoT) на основі хмарних технологій, на сьогоді, важко переоцінити. Український ІТ-ринок пропонує автономні системи, які є фундаментальними для більшості інформаційних підходів. Системи на основі Internet of Things, це комбінація з апаратного забезпечення (компонент та датчик), яке контролюється та управліється та програмного забезпечення (вихідний код, програми), які пов’язані між собою мережею, що, в свою чергу, дозволяє обмінюватися даними. Загалом, системи Internet of Things можуть бути присутні всюди для створення технічних та соціально-економічних можливостей з прямою інтеграцією між фізичним миром та комп’ютерними програмними системами. Однак, в контексті програмних IoT існує низка проблем, таких як проектування, безпека, захист, конфеденційність, управління та регулювання, які необхідно враховувати при проектуванні, моделюванні, розробці, розвитку та ефективному використанні систем, що застовано на Internet of Things.

Зарубіжний досвід використання платформи Internet of Things на основі хмарних технологій налічує десятки років та тисячі розробок. Моделі архітектури програмного забезпечення, ефективно використовуються на складних системах промислового виробництва. Архітектура програмного забезпечення для IoT спрямована на виявлення складнощів різнорідного обладнання, компонентів та мережевих протоколів для забезпечення безперебійної роботи, а також підвищення якості обчислень в системах IoT [1]. Наприклад, архітектурні компоненти (як модулі виконуваного коду) можуть забезпечити програмовані і стандартизовані інтерфейси для роботів побутової техніки, які можуть легко координувати один з одним за допомогою архітектурних роз'ємів (як передача повідомлень між модулями коду). Це

означає, що існуючі дослідження, кращі практики і принципи програмного забезпечення можуть використовуватися для моделювання, розробки, виконання та розвитку складних систем IoT, які задовольняють бажану функціональність, а також необхідну якість [2]. Проте, існує необхідність вийти за рамки існуючих досліджень для розробки архітектурних рішень на основі IoT щоб підтримати виникаючи проблеми для програмно-орієнтованих IoT [3-4].

В поточному десятилітті спостерігається стійке зростання досліджень і розробок щодо архітектурних рішень для вирішення різних завдань, які варіюються від специфічних аспектів проектування, експлуатації, управління та безпеки для програмного забезпечення IoT [5].

В.Ш. Гіоргізова-Гай, А.О. Шеренковський [1] докладно підійшли до розкляду питання використання шлюзів в системах IoT. Авторами виділено перелік головних функцій та основних характеристик шлюзів IoT і запропоновано критерії їх класифікації та порівняння.

Виробників обладнання для реалізації системи IoT розкриває Л. О'Доннелл [2].

Короткий огляд апаратних платформ, типових архітектурних рішень і послуг для корпоративних інформаційних систем наведно на офіційному сайті компанії Hewlett Packard [3]. Огляд є широким, опис кожної платформи вичерпний.

Ю.М. Лисецький, Д.І.Калбазов [4] розглянули IoT-технології в контексті перспектив її розвитку в Україні. Вчені прийшли до висновку, що незважаючи на те, що ця технологія добре зарекомендувала себе в США і розвинених європейських країнах, в Україні механізми економічної аргументації для її широкого впровадження ще не відпрацьовані, а обсяг коштів, що виділяються на моніторинг екологічного стану на державному і на муніципальному рівні недостатній.

Із зарубіжних авторів варто відзначити роботи M. Beshley, M. Klymash [5], Ademir F.da Silva, Ricardo L.Ohta [6] та інші.

Незважаючи на масштабність наукових досліджень у сфері управління безпекою інформаційних потоків мережі IoT за допомогою SDN, згадана тема залишається вивченою не повною мірою та потребує подальших досліджень.

1.2 Поняття інформаційних потоків

Інформаційні потоки – це шляхи передачі інформації, що забезпечують існування будь-якої системи. Повна, своєчасна і точна інформація (тобто добре налагоджений і організований інформаційний потік), підвищує продуктивність праці на 10-30%. Це процеси передачі інформації для забезпечення взаємозв'язку всіх ланок соціальної системи.

Існує два основних види інформаційних потоків:

- горизонтальні (між рівними за службовим положенням і статусом працівниками або групами працівників, наприклад, між начальниками відділів);
- вертикальні (між працівниками чи групами працівників, що знаходяться на різних рівнях ієрархії, наприклад, між начальником і підлеглим).

У свою чергу, вертикальні інформаційні потоки поділяються на спадні (від керівництва до рядових працівників по ієрархії) і висхідні (від нижчестоящих працівників до вищестоящих).

Кожен вид інформаційних потоків має свої особливості.

1. Горизонтальні інформаційні потоки

Найчастіше вони мають неформальний характер. Горизонтальні інформаційні потоки є найефективнішими, з комунікативної точки зору. У них зберігається приблизно 90% відомостей. Тобто втрата інформації при передачі таким шляхом мінімальна. Пояснюється це тим, що людям, які перебувають на одному рівні службової ієрархії, психологічно легше зрозуміти один одного, адже вони вирішують однотипні завдання і стикаються з подібними проблемами.

2. Спадні інформаційні потоки

Вони можуть бути і формальними, і неформальними. З точки зору їх комунікативної ефективності, ситуація виглядає наступним чином: чим більше передавальних ланок проходить спадна інформація, тим більше вона втрачається і змінюється. Йде об'єктивний процес спотворення отриманих відомостей. У практичній роботі менеджер повинен виходити з того, що кожне передавальне ланка «забирає» до 50% інформації, що надходить.

Парадокс полягає в тому, що інформацію, яка отримується зверху не приховується і не спотворюється кимось спеціально або свідомо; просто повноті передачі перешкоджають комунікативні бар'єри. При низхідних інформаційних потоках спостерігається ефект «зіпсованого телефону».

І навпаки: повна, своєчасна і точна інформація (тобто добре налагоджений і організований інформаційний потік), підвищує продуктивність праці на 10-30%.

3. Висхідні інформаційні потоки

Вони вкрай рідко бувають неформальними, це не потребує роз'яснення. Спотворення інформації в такому потоці може досягати 90%. Найцікавіше, що міститься в них інформація найменше аналізується. Якщо на підприємстві, в фірмі чи установі не організований приплив ідей знизу, значить, можливості для його інноваційного розвитку значно обмежені.

І навпаки: добре налагоджений процес надходження ідей від підлеглих в значній мірі підвищує ефективність роботи підприємства. Як же організувати висхідний інформаційний потік, як налагодити приплив ідей знизу? Для цього існує кілька способів. Однак головний стратегічний напрямок полягає не в посиленні інтенсивності, а у встановленні конфіденційності. Неформальна, конфіденційна, інформація найменше спотворюється.

Отже, для поліпшення висхідних потоків можна використовувати:

1. Систему дій, що позначаються терміном «політика відкритих дверей». Це – готовність керівника будь-якого рангу вислуховувати пропозиції рядових працівників.

2. Систему дій, звану «виведенням управління за межі кабінету». Ця система називається ще «видимим управлінням», «управлінням шляхом обходу робочих місць».

Модифікований спосіб «видимого управління» отримав назву «список особистих подій співробітників за 24 години».

При використанні цих двох тактик ефективність висхідних інформаційних потоків зростає до 40%, а це - хороший резерв не тільки для вдосконалення стилю управління, але і для підвищення якості роботи підприємства в цілому.

Для того щоб зробити управлінське спілкування повноцінним і ефективним, а також щоб перетворити його в фактор успішного управління, необхідно дотримуватися двох умов:

- організувати інформаційні потоки;
- на кожному управлінському «поверсі» мати достатньо часу для обробки інформації, що надходить і її аналізу.

Зовнішній інформаційний потік – це інформація, яка надходить у фірму (підприємство, установа) ззовні і йде з фірми зовні. У тому, що такий процес відбувається, не варто сумніватися: адже жодна соціальна система не може існувати без обміну інформацією із зовнішнім світом. Такі потоки теж мають специфічні особливості.

По-перше, їх майже неможливо контролювати. По-друге, зовнішній інформаційний потік майже не піддається свідомому регулюванню. Єдиний спосіб управління ним - використовувати такий потік для створення «образу підприємства», його іміджу в очах громадської думки.

1.3 Інтернет речей: сутність, поняття, генезис

Інтернет речей (Internet of Things, IoT) – це концепція і парадигма, яка розглядає повсюдно присутність різних фізичних об'єктів («речей») в навколишньому середовищі. Термін «Інтернет речей» визначено як динамічну глобальну мережеву інфраструктуру з можливістю самонастроювання на основі стандартних і сумісних протоколів зв'язку, де фізичні та віртуальні

«речі» мають ідентифікатори, фізичні атрибути, використовують інтелектуальні інтерфейси і інтегруються в інформаційну мережу [1].

Протягом останнього десятиліття Інтернет речей проникав в наше життя тихо і поступово, перш за все завдяки наявності систем бездротового зв'язку (наприклад, RFID, Wi-Fi, 4G, IEEE 802.15.x), які все частіше використовуються в якості рушійної сили для розвитку технології інтелектуального контролю та управління додатками [2]. Концепція IoT включає в себе безліч різних технологій, послуг, стандартів і сприймається як наріжний камінь на ринку інформаційно-комунікаційних технологій (ІКТ) принаймні на найближчі десять років. З логічної точки зору, система IoT може бути представлена як сукупність спільно взаємодіючих інтелектуальних пристроїв. З технічної точки зору, IoT може використовувати різні шляхи обробки даних, комунікації, технології та методології, ґрунтуючись на їх цільовому призначенні. Наприклад, система IoT може скористатися наявними можливостями бездротової сенсорної мережі (WSN), яка збирає екологічно значиму інформацію про навколишнє середовище [3]. Високий рівень неоднорідності в поєднанні з широкою гамою систем IoT, як очікується, збільшить число загроз безпеки власників пристроїв, які все частіше використовуються для взаємодії людей, машин і речей в будь-який варіації. Традиційні заходи забезпечення безпеки і дотримання конфіденційності не можуть бути застосовані до технологій IoT, зокрема, через їх обмежену обчислювальну потужність. Крім того, велика кількість підключених пристроїв породжує проблему масштабованості. У той же час для досягнення визнання з боку користувачів необхідно в обов'язковому порядку забезпечити дотримання безпеки, конфіденційність і модель довіри, які підходять для контексту IoT [4-6].

Для запобігання несанкціонованого доступу користувачів (тобто людей і пристроїв) до системи повинні використовуватися механізми аутентифікації і авторизації, гарантована безпека, конфіденційність і цілісність персональних даних. Щодо персональних даних користувачів і інформації повинні

забезпечуватися захист і конфіденційність, перш за все тому, що пристрої мають до неї доступ і здатні управляти нею (наприклад, відомості про звички користувачів). Нарешті, довіра (надійність, англ. Trust) – це основна проблема, оскільки IoT-середовище характеризується різними типами пристроїв, які повинні обробляти дані відповідно до потреб і прав користувачів.

Звернемо увагу, що адаптація і самовідновлення грають ключову роль в IoT інфраструктурах, які повинні бути в змозі протистояти несподіваним змінам у навколишньому середовищі. Відповідно, до питань конфіденційності та безпеки слід ставитися з високим ступенем гнучкості. Поряд з традиційними рішеннями для забезпечення безпеки необхідне використання спеціальних механізмів, вбудованих в самі пристрої з метою оперативної діагностики, ізоляції та профілактики порушень [7].

Що стосується аутентифікації, підхід, представлений в [8], передбачає використання механізму інкапсуляції, який настроюється користувачем, а саме протокол прикладного рівня для IoT під назвою – «інтелектуальна служба забезпечення безпеки» (англ. Intelligent Service Security Application Protocol). Він поєднує в собі крос-платформні зв'язки з шифруванням, підписом і аутентифікацією для підвищення ефективності розробки додатків IoT шляхом створення системи захищеного зв'язку між різними речами.

В роботі [9] представлена перша повністю реалізована двостороння схема перевірки справжності для IoT на основі існуючих стандартів, зокрема, протокол датаграм безпеки транспортного рівня (англ. Datagram Transport Layer Security, DTLS), який розташовується між транспортним і прикладним рівнями. Ця схема заснована на криптографічному алгоритмі RSA і призначена для IPv6 з використанням стандарту 6LoWPANs (англ. IPv6 over Low power Wireless Personal Area Networks) [10]. Аналіз результатів, заснованих на реальних системах IoT, показує, що така архітектура забезпечує цілісність повідомлення, конфіденційність, енергоефективність, низькі значення затримки пакетів і навантаження на пам'ять.

Щодо конфіденційності і цілісності в [11] наведено аналіз того, як існуючі системи управління ключами можуть бути застосовані в контексті IoT. Це дозволяє класифікувати протоколи систем управління ключами (англ. Key Management System, KMS) за чотирма основними категоріями: структура пулу ключів, математична база, механізм взаємодії і структура відкритого ключа. В роботі [12] автори стверджують, що більшість протоколів KMS не підходять для IoT. Однак протоколи KMS придатні для сценаріїв, в яких обчислювальні потужності є досить низькими в порівнянні з використанням криптографії з відкритим ключем (англ. Public Key Cryptography, PKC). Але для таких схем необхідне введення декількох контрзаходів для управління пристроєм аутентифікації і щоб уникнути MITM-атаки (англ. Man In The Middle).

Більш практичний підхід [13] пропонує модель передачі зі схемами шифрування підпису, в якій розглядаються вимоги безпеки IoT (тобто анонімність, надійність і стійкість до атак) за допомогою ONS-запитів (англ. Object Naming Service). Однак, з точки зору стійкості до атак, результати моделі передачі даних є дуже слабкими в зв'язку з використанням шифрування на базі «точка-точка» (англ. Hop-by-hop). Як і раніше відсутнє унікальне і чітко визначене рішення, яке може гарантувати конфіденційність в IoT. У цьому контексті багато зусиль було докладено для WSN (англ. WSN - Wireless Sensor Network) [14, 15].

В рамках WSN аутентифікація користувача і схема узгодження ключа для гетерогенних бездротових сенсорних мереж також запропонована, наприклад, в [17]. Це рішення дозволяє віддаленому користувачеві безпечно домовитися про сеансовий ключ з сенсорним вузлом за допомогою протоколу розподілу ключів. Таким чином, він забезпечує взаємну аутентифікацію між користувачами, сенсорними вузлами і шлюзовими вузлами (англ. Gate way node, GWN). Для того щоб застосувати таку схему для архітектури з обмеженими ресурсами, використовуються тільки прості хеш і XOR обчислення.

Метод перевірки автентичності і контроль доступу, представлений в [18], спрямований на створення ключа сеансу із застосуванням еліптичної криптографії (англ. Elliptic Curve Cryptography, ECC). Крім того, запропонований механізм захисту даних в хмарних сховищах, заснований на поєднанні «класичної» проблеми Діффі-Хеллмана і проблеми дискретного логарифмування в групі точок еліптичної кривої. Відзначається, що протокол, заснований на еліптичних кривих, має невеликий розмір ключа без шкоди криптостійкості, що робить еліптичну криптографію привабливою для використання в тих областях, де існують проблеми з-за обмеження пам'яті і обчислювальних потужностей.

Управління доступом відноситься до дозволів в галузі використання ресурсів, призначених для різних суб'єктів в мережі IoT. В [19] визначені два суб'єкти: власники даних і збирачі даних. Користувачі і речі, як власники даних, повинні дозволяти передавати тільки відомості, які необхідні для виконання конкретного завдання. У той же час збирачі даних повинні вміти ідентифікувати або підтвердити справжність (аутентифікувати) користувачів речей як законних власників даних, від яких вона збирається.

У IoT мають справу з обробкою потокових, а не дискретних даних, як в традиційних системах. Основні проблеми в цьому контексті відносяться до продуктивності і тимчасових обмежень. Зокрема, потік даних інтенсивніше, ніж в традиційних системах управління базами даних (СУБД). Кілька робіт присвячено цим аспектам.

В [20] увага зосереджена на рівні, відповідальному за отримання і зберігання інформації. Велика кількість вузлів авторизованих користувачів використовує широкий спектр різних типів даних відповідних рівнях конфіденційності та безпеки. Тому в роботі представлена ієрархічна схема управління доступом для цього рівня. Схема враховує обмежену обчислювальну потужність і ємність пристрою зберігання. Кожному користувачеві і / або вузла дається тільки один ключ; інші необхідні ключі отримані за допомогою детермінованого алгоритму деривації ключа (англ.

deterministic key derivation algorithm), підвищуючи рівень безпеки (так як обмін ключів обмежений) і скорочуючи витрати на зберігання для безлічі вузлів.

Інтернет речей концептуально належить до мереж наступного покоління, тому його архітектура багато в чому схожа з відомою чотиришаровою архітектурою NGN. IoT складається з набору різних інфокомунікаційних технологій, що забезпечують функціонування Інтернету речей, і його архітектура показує, як ці технології пов'язані один з одним.

Архітектура IoT включає чотири функціональних рівня (рис. 1.1), описаних нижче.

1. Рівень сенсорів та сенсорних мереж.

Самий нижній рівень архітектури IoT складається з «розумних» (smart) об'єктів, інтегрованих з сенсорами (датчиками). Сенсори реалізують з'єднання фізичного та віртуального (цифрового) світів, забезпечуючи збір і обробку інформації в реальному масштабі часу. Мініатюризація, яка призвела до скорочення фізичних розмірів апаратних сенсорів, дозволила інтегрувати їх безпосередньо в об'єкти фізичного світу. Існують різні типи сенсорів для відповідних цілей, наприклад, для вимірювання температури, тиску, швидкості руху, місця розташування та ін. Сенсори можуть мати невелику пам'ять, даючи можливість записувати деяку кількість результатів вимірювань. Сенсор може вимірювати фізичні параметри контрольованого об'єкта/явища і перетворити їх в сигнал, який може бути прийнятий відповідним пристроєм. Сенсори класифікуються згідно з їх призначенням, наприклад, сенсори навколишнього середовища, сенсори для тіла, сенсори для побутової техніки, сенсори для транспортних засобів і т. д.

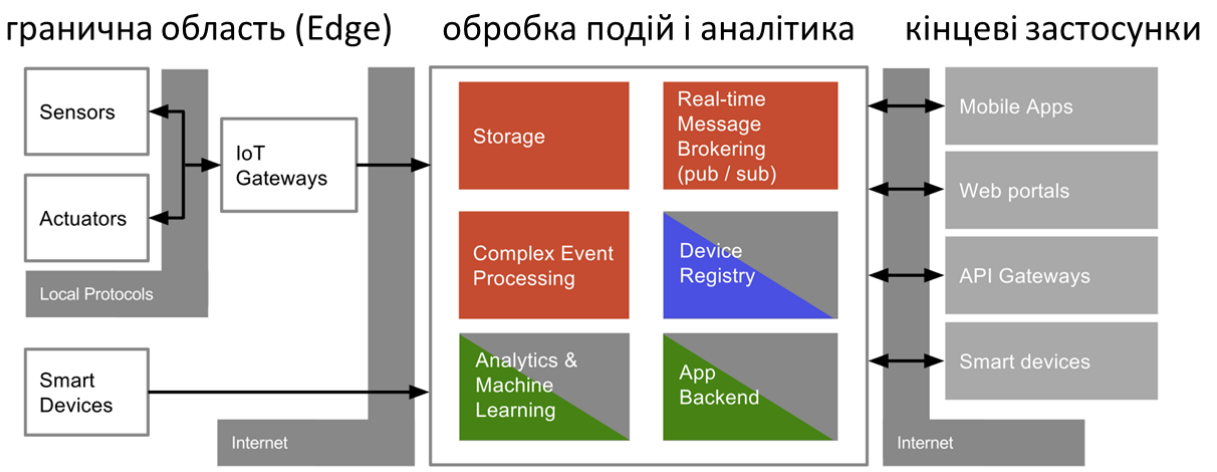


Рис. 1.1 Архітектура IoT

Більшість сенсорів потребує з'єднання з агрегатором сенсорів (шлюзом), які можуть бути реалізовані з використанням локальної обчислювальної мережі (LAN, Local Area Network), таких як Ethernet і Wi-Fi або персональної мережі (PAN, Personal Area Network), таких як ZigBee, Bluetooth і ультраширокополосного бездротового зв'язку на малих відстанях (UWB, Ultra-Wide Band). Для сенсорів, які не вимагають підключення до агрегатору, їх зв'язок з серверами/додатками може надаватися використанням глобальних бездротових мереж WAN, таких як GSM, GPRS і LTE.

Сенсори, які характеризуються низьким енергоспоживанням і низькою швидкістю передачі даних, утворюють широко відомі бездротові сенсорні мережі (WSN, Wireless Sensor Network). WSN набирають все більшу популярність, оскільки вони можуть містити набагато більше сенсорів з підтримкою роботи від батарей і охоплюють великі площі.

2. Рівень шлюзів і мереж.

Великий обсяг даних, створюваних на першому рівні IoT численними мініатюрними сенсорами, вимагає надійної і високопродуктивної провідної або бездротової мережевої інфраструктури в якості транспортного середовища. Існуючі мережі зв'язку, що використовують різні протоколи, можуть бути використані для підтримки міжмашиних комунікацій M2M та їх додатків. Для реалізації широкого спектру послуг і додатків в IoT необхідно

забезпечити спільну роботу безлічі мереж різних технологій і протоколів доступу в гетерогенній конфігурації. Ці мережі повинні забезпечувати необхідні значення якості передачі інформації, і перш за все по затримці, пропускної спроможності та безпеки. Цей рівень складається з конвергентної мережевої інфраструктури, яка створюється шляхом інтеграції різнорідних мереж в єдину мережеву платформу. Конвергентний абстрактний мережевий рівень у IoT дозволяє через відповідні шлюзи декільком користувачам використовувати ресурси в одній мережі незалежно і спільно без шкоди для конфіденційності, безпеки і продуктивності.

3. Сервісний рівень

Сервісний рівень містить набір інформаційних послуг, спрямованих автоматизувати технологічні і бізнес-операції в IoT: підтримки операційної та бізнес діяльності (OSS/BSS, Operation Support System/Business Support System), різної аналітичної обробки інформації (статистичної, інтелектуального аналізу даних і текстів, прогностична аналітика та ін), зберігання даних, забезпечення інформаційної безпеки, управління бізнес-правилами (BRM, Business Rule Management), управління бізнес-процесами (BPM, Business Process Management) і ін.

4. Рівень додатків

На четвертому рівні архітектури IoT існують різні типи додатків для відповідних промислових секторів і сфер діяльності (енергетика, транспорт, торгівля, медицина, освіта та ін.). Додатки можуть бути «вертикальними», коли вони є специфічними для конкретної галузі промисловості, а також «горизонтальними», (наприклад, управління автопарком, відстеження активів та ін), які можуть використовуватися в різних секторах економіки.

Існують кілька еталонних архітектур і моделей і для M2M і IoT систем. Розглянемо архітектуру ETSI M2M високого рівня.

Архітектура високого рівня (рис.1.2) є комбінацією функціонального і топологічного огляду, який показує деякі функціональні групи, пов'язані з частинами фізичної інфраструктури (наприклад, пристроїв M2M, шлюзи) в

той час як інші функціональні групи не мають конкретного топологічного розміщення. Основними елементами архітектури M2M систем є мережевий домен і домен пристроїв і шлюзів.

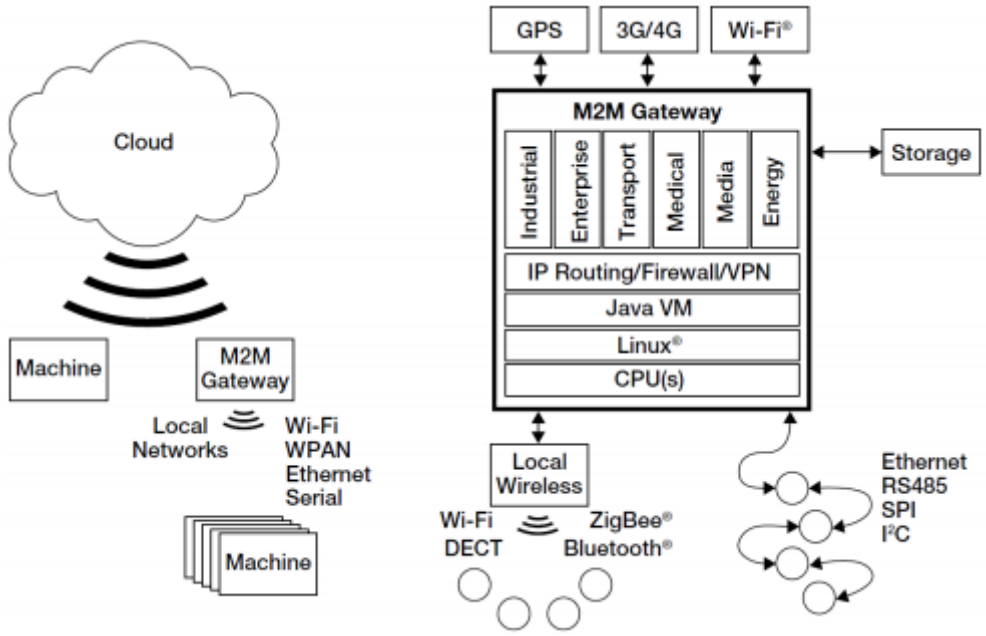


Рис. 1.2 Архітектура ETSI M2M високого рівня

Крім зазначених доменів до складу мережі M2M входять відповідна мережа доступу і транспортна мережа, які будуються на основі мереж 3GPP і NGN мереж.

Мережі доступу (Access Network) дозволяють домену пристроїв M2M забезпечувати з'єднання з ядром мережі M2M (базовою мережею). Функціональні можливості мереж доступу M2M базуються на можливостях існуючих мереж доступу (xDSL, HFC, PLC, VSAT, GERAN, UTRAN, LTE, W-LAN і WiMAX) та дозволяють розширити як перелік послуг, так і їх можливості.

Транспортна мережа (Core Network) забезпечує транспортування даних між мережевим доменом і доменом додатків. Функціональні можливості трасування мереж в мережах M2M базуються на можливостях існуючих мереж трасування і так само, як мережі доступу, дозволяють розширити перелік послуг M2M і їх можливості.

Базова мережа M2M (M2M Service Capabilities) надає функціональні можливості IP-з'єднання елементів мережі M2M, сервісні та мережеві функції управління, між мережеву взаємодію, роумінг та забезпечує безпеку мережі. Функціональні можливості базової мережі M2M ґрунтуються на відповідних функціональних можливостях існуючих базових мереж 3GPP CN (наприклад, GPRS, EPC), ETSI TISPAN CN.

Пристрої M2M (M2M Device) дозволяють швидко скористатися послугами M2M і функціями доменної мережі. Пристрій M2M може бути пов'язаний з мережею доступу або безпосередньо, або через локальну мережу M2M і шлюз M2M.

Локальні мережі M2M (M2M Area Network) надають з'єднання між пристроями M2M і шлюзами M2M з використанням PAN-технологій (IEEE 802.15, SRD, UWB, Zigbee, Bluetooth) або локальних мереж (PLC, M-BUS, Wireless M-BUS).

Шлюзи M2M (M2M Gateway) забезпечують пристроям M2M гарантовану міжмережеву взаємодію і підключення до мережі і прикладних доменів. Шлюз M2M може використовуватися для різних додатків пристроїв M2M. Функціонально шлюз M2M може бути об'єднаний в одному модулі с пристроєм або групою пристроїв M2M.

Функціональні можливості мережі M2M можуть бути як спеціальними, що підтримують додатки M2M, так і загальними, що підтримують загальномережеві можливості: збір та агрегацію даних, доставку багато адресних повідомлень і ін.

Однак є фактори, здатні уповільнити розвиток Інтернету речей. Одним з найважливіших вважається відсутність прийняття загальних стандартів. У структурі головного європейського органу зі стандартизації в області телекомунікацій – Європейського інституту стандартизації електрозв'язку (ETSI) в 2009 році був створений технічний комітет ТК M2M. За час роботи ТК M2M / ETSI була розроблена нормативно-технологічна база, що включає кілька технічних звітів і стандартів ETSI, які визначили вимоги до

функціональної архітектури мереж M2M, пристроїв, інтерфейсів і основних бізнес-моделей послуг M2M.

В рамках діяльності Комітету з електронних комунікацій ECC / CEPT адміністрацій зв'язку країн Європи прийнято ряд рішень і рекомендацій по використанню радіочастотного спектру для пристроїв M2M [3, 4]

1.4 Програмно-конфігурована мережа

Можливість працювати буквально де завгодно істотно підвищує продуктивність і мотивує свідомих співробітників на багато що. Сьогодні користувачі можуть отримувати доступ до даних і додатків з будь-якого місця: в офісі, вдома, в аеропорту, в готелі. Причому використовувати для цього найрізноманітніші пристрої: ноутбук, планшет, смартфон і, використовуючи будь-які технології провідні мереж Ethernet, WiFi або 3G / 4G. Корпоративні додатки переносяться з фізичних серверів на віртуальні машини або навіть в хмари.

Хмарні технології докорінно змінюють основну модель витрат компаній, перетворюючи частину витрат на створення IT-інфраструктури з капітальних витрат в операційні і допомагають гнучко нарощувати додаткові ресурси або потужності на вимогу або в міру зростання бізнесу. Робочі столи співробітників стають віртуальними, перестаючи бути прив'язаними до чорних скриньок конкретних комп'ютерів. Набагато ефективніше вирішуються питання ліцензування програмного забезпечення та його своєчасного оновлення. Однак при цьому, хмарні технології і створюють певні проблеми, істотно ускладнюючи життя IT-фахівцям в тих випадках, коли потрібно зрозуміти, з чим пов'язана низька продуктивність сервісів і на чиєму боці виникла проблема.

Термін «консьюмеризація IT» в основному означає тенденцію використання співробітниками своїх особистих пристроїв (BYOD) для виконання робочих функцій. Для цього відділ IT повинен вирішити задачу ефективної прив'язки різних гаджетів до корпоративної мережі, в тому числі – і особистих ноутбуків (BYOC). Крім того, при впровадженні BYOD і / або

BYOC служба IT буде змушена здійснювати підтримку не тільки корпоративних пристроїв, але і особистих пристроїв. На більшість гаджетів встановлені в тому числі і сторонні додатки, які автоматично оновлюються в тлі при підключенні до будь-якої мережі, і таким чином будуть конкурувати за IT ресурси нарівні з корпоративними пристроями. На жаль, на даному етапі не всі сучасні рішення з моніторингу IT-інфраструктури готові надати реальну допомогу та підтримку IT-фахівцям в забезпеченні питань безпеки і продуктивності такого спільного використання.

Ефективне впровадження всіх нових тенденцій в рамках існуючої концепції побудови мереж – завдання не з простих. Адже по суті, мережі протягом останніх років концептуально майже не змінювалися – росли швидкості і з'являлися нові протоколи, але принципи управління і передачі трафіку практично не змінювалися (якщо не сказати відверто - ускладнювалися і далеко не завжди це ускладнення призводило до позитивних результатів). Типовий підхід в організації середньостатистичної сучасної корпоративної мережі: кожен елемент налаштовується і адмініструється відокремлено, якщо виникає проблема з продуктивністю, то пристрій просто змінюється на більш інноваційний. Підтримувати нові технології, враховуючи нереальну швидкість їх появи і розробки, з використанням старих принципів стало практично неможливо. Наприклад, якщо вирішимо запустити нову віртуальну машину сьогодні і перенести на неї додаток, то перенастроювання списків контролю доступу на всіх пристроях корпоративної мережі може зайняти кілька днів, що неприпустимо.

Концепція програмно-визначених мереж (SDN) грунтовно змінює принципи функціонування мереж і їх управління. У швидко мінливому сучасному світі саме мережі передачі даних були названі «тонкою ланкою», яке обмежує зростання продуктивності додатків по мірі зростання кількості мобільних користувачів, масштабування віртуальних середовищ, формування кластерів для Великих Даних. У SDN мережах завдання комутації трафіку і завдання управління строго розділені. Вся логіка управління централізується і

передаються контролеру. Комутатор у концепції SDN - досить примітивний пристрій, який відповідає тільки за перемикання пакетів на підставі дуже простих правил. Контролер SDN управляє всіма комутаторами в мережі і програмує кожен з них для правильної передачі трафіку. Централізація логіки управління дозволяє програмувати мережу як єдине ціле і спростити операційну модель великих корпоративних мереж, які занадто статичні на даний момент і не відповідають сучасному бізнесу, з властивими йому мобільністю користувачів / пристроїв / додатків, розподілом додатків між віртуальними машинами і інтенсивним обміном даними.

Незалежне від виробника управління всіма пристроями з єдиного центру суттєво спрощує конфігурацію і експлуатацію мережі. Завдяки контролеру з розширеними API інтерфейсами, вся мережа стає подібною одному великому логічному комутатору. Протокол OpenFlow – один з найбільш універсальних протоколів комунікації контролерів і комутаторів на сьогоднішній день надає стандартний підхід до програмування таблиць комутації, в яких основним об'єктом є потік даних. Однак в той час як OpenFlow дозволяє контролеру програмувати комутатори, він не визначає, як контролеру реагувати і відповідати на виклики, пов'язані з хмарами, BYOD, BYOC, віртуалізацією.

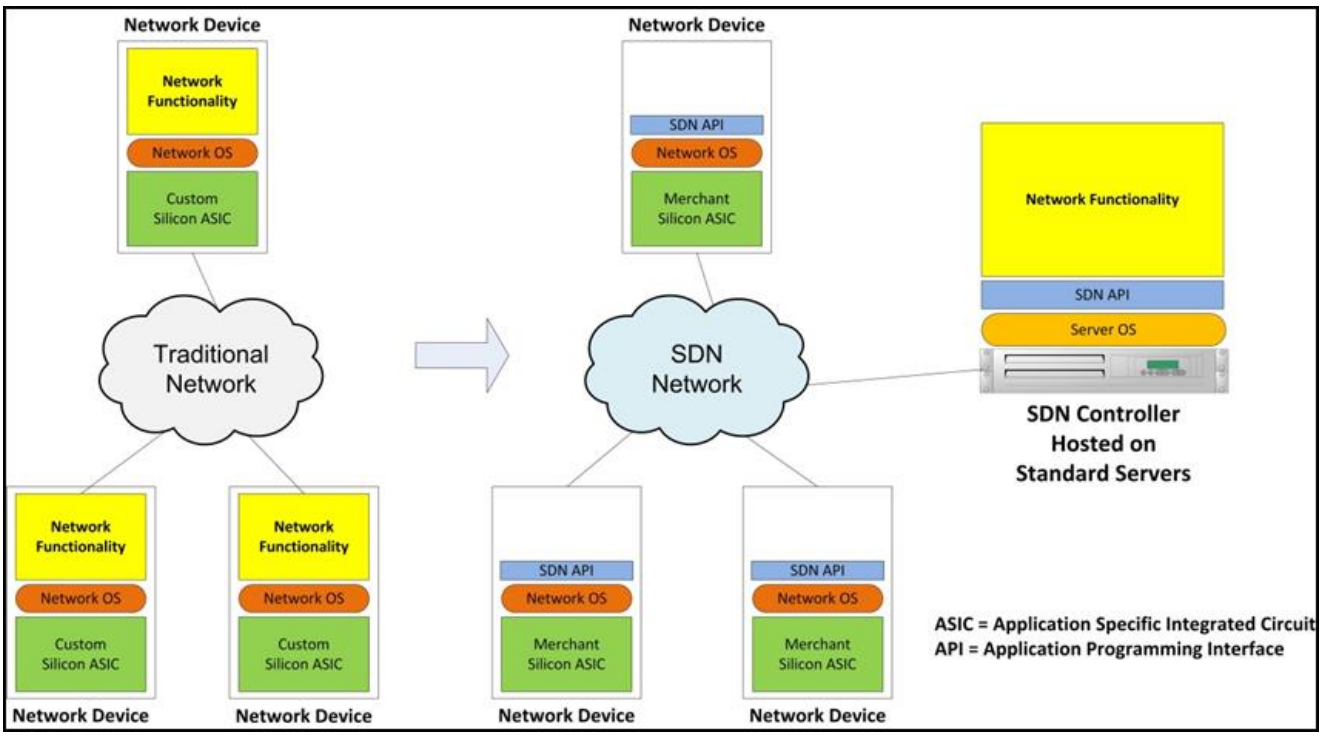


Рис. 1.3 Архітектура SDN

Рішення будь-яких проблеми з продуктивністю мережі, та й просто її роботою, покладені на контролер і додатки, які на ньому запущені. Саме набір таких додатків і відрізняє різні впровадження SDN, а також рішення різних виробників. Тому під парасолькою SDN на даний момент розвиваються інші технології, які поки прив'язані до того чи іншого виробника.

Слідом за віртуалізацією серверів і додатків прийшла черга мереж. Розроблені 35 років тому класичні віртуальні мережі VLAN, що працюють на другому рівні моделі OSI були відмінним рішенням для логічного угруповання пристроїв і управління обміном інформацією між ними. Але даний підхід має обмеження – з його допомогою можна організувати 4094 мережі і неможливо перенести віртуальну машину через кордони канального рівня. Таким чином виникла модель створення накладених віртуальних мереж поверх існуючої фізичної IT інфраструктури.

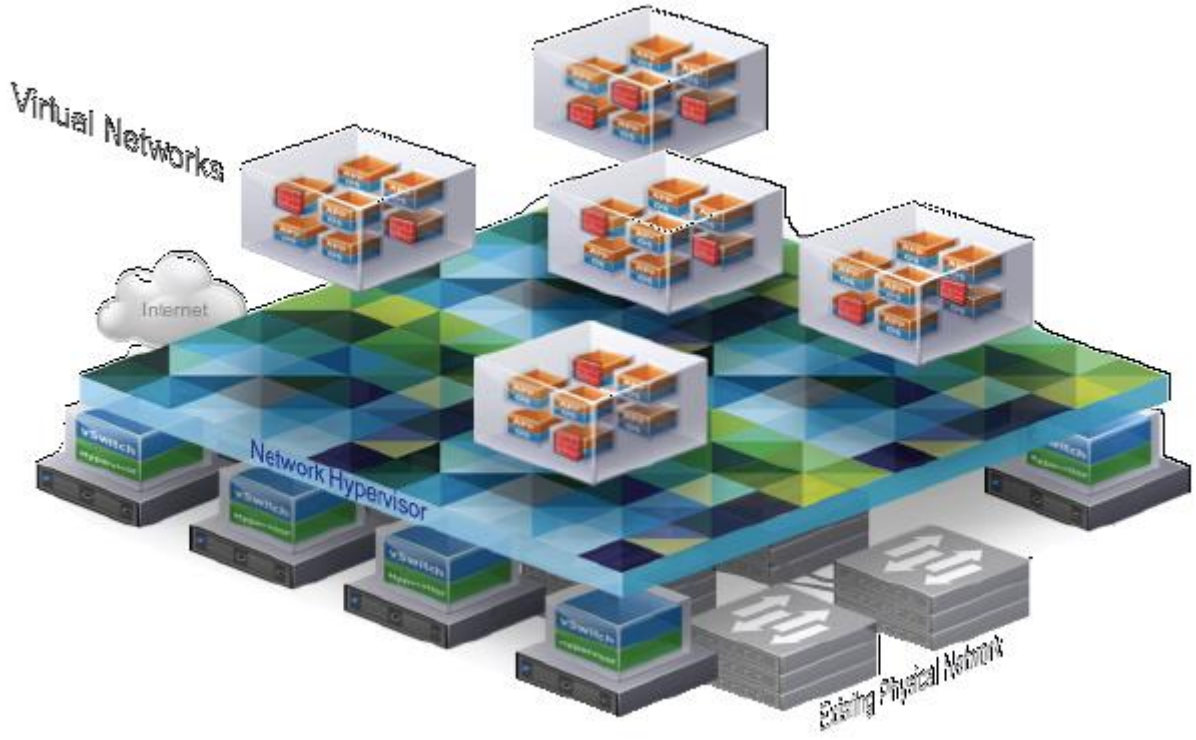


Рис. 1.4 Накладені віртуальні мережі

У якості найпоширеніших протоколів побудови накладених (оверлейних) мереж можна привести VXLAN (компанія VMware) і NVGRE (компанія Microsoft). Всі протоколи мають на увазі наявність віртуального комутатора на базі гіпервізора і термінування тунелів у віртуальних вузлах. Що дозволяє будувати логічні мережі на канальному рівні в рамках вже існуючих мереж рівня 3 моделі OSI. Віртуалізація мережі відповідає на виклики мобільності і розрахованого на багато користувачів використання, але створює додаткові проблеми, пов'язані з питаннями моніторингу, управління і безпеки як для самої фізичної інфраструктури, так і накладених віртуальних мереж. Основні проблеми з яким доведеться зіткнутися – це моніторинг та контроль за синхронізацією управління мережею (фізичною і накладеною) і управління потоками даних.

Рішення на основі SNMP для моніторингу всієї мережі, швидше за все не будуть затребувані, тому що SDN-мережі будуються на основі простих пристроїв комутації і весь розум зосереджений в контролері, тому основну інформацію через API інтерфейси можна буде легко зняти. А ось проблему синхронізації і можливих збоїв в спілкуванні контролер-комутатор доведеться вирішувати за допомогою рішень для аналізу продуктивності сервісів і мережі на основі глибокого аналізу реального трафіку.

Уявімо велику програмну мережу, яка визначається. Все управління здійснюється контролером, і він повинен бути синхронізований з усіма комутаторами і оперативно оновлювати інформацію. На папері виглядає дивовижно і легко написати, що все буде літати і працювати як треба, але реальне життя складніше віртуального і проблеми будуть і рости з ростом SDN мережі. Зростання SDN мережі і кількість обладнання буде приводити до збільшення часу для синхронізації контролера і комутаторів при внесенні змін в конфігурацію мережі. Це може бути пов'язано з різними чинниками, такими як затримка між контролером і комутатором, втрати пакетів в каналах зв'язку, обладнання від різних виробників, яке має різні розміри внутрішніх таблиць комутації, ну або як мінімум наявність багів і проблем в програмному або

апаратному забезпеченні. Залежно від впровадження, комутатори можуть розсинхронізуватися з контролером і не відновити зв'язок протягом деякого періоду часу. У такій ситуації передбачити поведінку мережі дуже складно. Для того, щоб мінімізувати такі ситуації необхідно моніторити трафік між комутаторами, щоб переконається, що мережа працює як планувалося в рамках того, що вважається нормальним. Це завдання буде можливо вирішити шляхом кореляції інформації по потокам даних на рівні комутаторів і налаштувань на рівні контролера. Дана інформація може бути корисна не тільки для вирішення завдань моніторингу продуктивності, але і для забезпечення безпеки SDN мережі. А також може використовуватися як зворотний зв'язок для внесення змін в налаштування через контролер в комутатори для відновлення очікуваної поведінки мережі.

Створення віртуальних мереж і в минулому і в майбутньому пов'язано з додаванням додаткових заголовків в пакети, що утруднює аналіз трафіку за допомогою рішень на коліні (типу ноутбук і аналізатор трафіку). Також не всі існуючі аналізатори можуть коректно відпрацьовувати трафік і видалення заголовків, які відносяться до VXLAN, NVGRE і т.д. В даному випадку можуть бути корисні брокери мережевих пакетів, які оперативно оновлюють свої функціональні можливості в частині аналізу нових видів протоколів і інкапсуляцій, в тому числі і для підтримки SDN мереж. Створення та видалення віртуальних каналів і оверлейних мереж відбувається на рівні гіпервізора і на рівні фізичної інфраструктури цей процес буде неможливо проконтролювати, що робить пошук несправностей і управління продуктивністю каналів зв'язку дуже складним. Наприклад, якщо пакет даних був відправлений з однієї віртуальної машини на іншу з використанням VXLAN і не дійшов до адресата, то причини можуть бути: в гіпервізорі; у відправнику; в контролері SDN мережі (невірний маршрут); у одержувачі; в базовій фізичній мережі. І нарешті, поділ потоків управління і користувача на рівні накладеної мережі і на рівні фізичної, вимагає контролю з можливістю кореляції, щоб бачити, як одна мережа впливає на іншу.

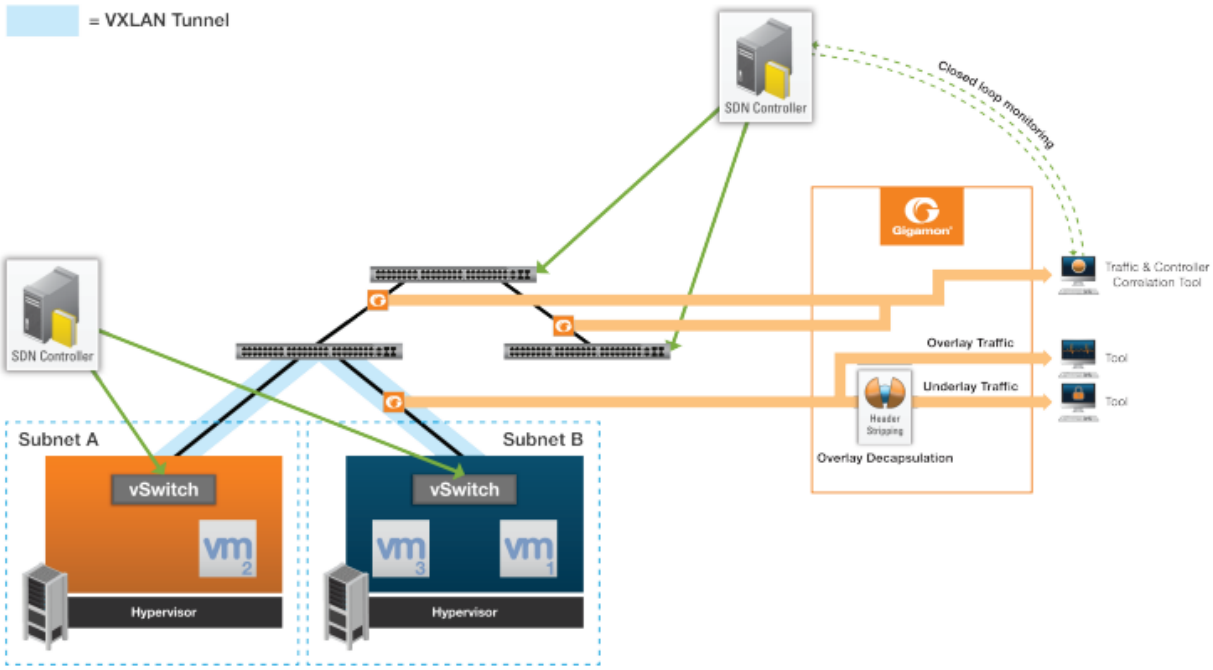


Рис.1.5 Схема ефективного моніторингу мереж SDN

Таким чином, для забезпечення ефективного моніторингу мереж SDN та фізичної інфраструктури необхідні сучасні рішення, які підтримують всі нові протоколи і інкапсуляції. Основна ідеологія SDN мережі – зробити мережу розумною і недорогою, тому система моніторингу продуктивності і безпеки, також як і управління мережею, повинна бути встановлена в одному місці. Таким чином, всі розподілені системи моніторингу замінюються на мережу знімання інформації за допомогою відгалужувачів трафіку.

Відгалужувачі трафіку встановлюються в мережі і надають доступ до реального трафіку. Далі маркіруючи трафік, доставляють його в центр для обробки і аналізу системами моніторингу або безпеки і видачі зворотного зв'язку для коректування налаштувань комутаторів через контролер. Компанія Gigamon дала назву своїй філософії Unified Visibility Fabric, а компанія VSS Monitoring - Unified Visibility Plane:

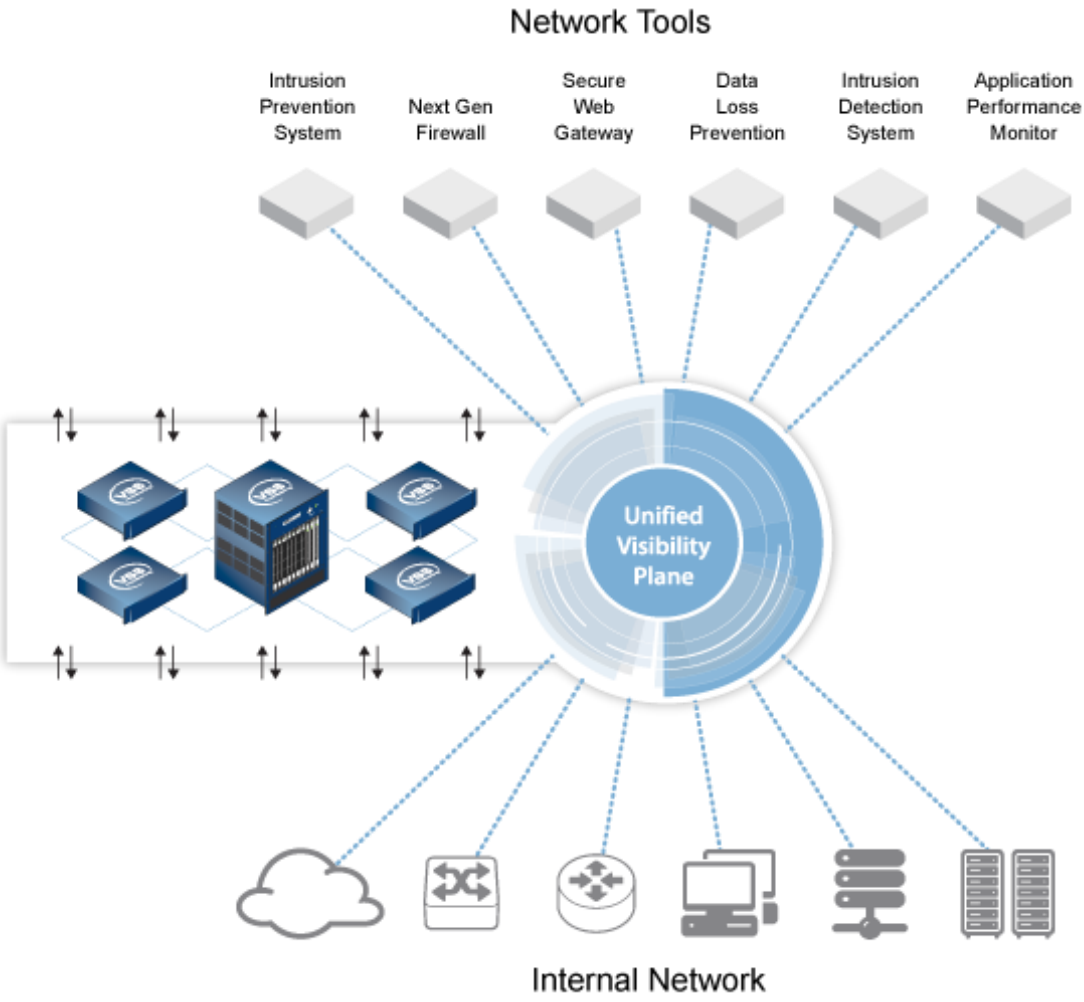


Рис.1.6 Схема встановлення відгалужувачів трафіку SDN

Але суті це не міняє, і система моніторингу стає відірваною від фізичної інфраструктури мережі, гнучко управляється через єдиний інтерфейс користувача і гарантовано приносить трафік для його обробки. Таким чином, буде дотримана і економічна складова, яку несе SDN мережа і можливості повного контролю продуктивності, які властиві традиційним мережам.

1.5 Проблематика дослідження та постановка завдань

Традиційне управління мережами зазвичай вимагає нлаштування кожного пристрою, що підключається до мережі окремо. Наприклад, конфігурація списку контролю доступу віртуальної частини локальної мережі (VLAN access control list) на декількох комутаторах Cisco неминуче тягне за собою вхід на кожен і виконання необхідних налаштувань. Подібний підхід успішно працював в минулому, але може вимагати значних витрат часу, коли

організації додадуть в мережі пристрої, принесені співробітниками, і численні хмарні сервіси. SDN може допомогти, тому що мета управління мережею – дозволяти різним пристроям підключатися до мереж і використовувати їх ресурси з обмеженнями, заснованими на принципах «хтось що-де-як-чому » при кожному підключенні. Це вимагає постійних застосувань політик серед всіх пристроїв. Надалі, адміністратор, який змінює політики, змушений проводити години очікування, роблячи зміни в кожному пристрої окремо, і ці зміни повинні узгоджуватися по всьому підприємству. Ось в чому роль SDN. Вони надають узгоджене, відносно швидке управління мережами, дозволяючи зміни у всій мережі з єдиної консолі управління.

Метою даної дипломної роботи є дослідження методів управління безпекою інформаційних потоків мережі IoT за допомогою SDN.

Завданнями дослідження є:

- проектування програмно-конфігурованої мережі на базі IoT;
- розкриття моделі управління безпекою інформаційних потоків мережі IoT;
- розробка алгоритму управління безпекою інформаційних потоків мережі IoT за допомогою SDN;
- наведення методології визначення ефективності управління безпекою інформаційних потоків мережі IoT за допомогою SDN;
- розкриття ефективності управління безпекою інформаційних потоків мережі IoT за допомогою SDN.

Висновки

У рамках першого розділу здійснено теоретико-методологічний аналіз методів управління безпекою інформаційних потоків мережі IoT за допомогою SDN.

У 2019 обсяг світового ринку програмно-визначених мереж і дата-центрів (технології SDN, SD-WAN і SDDC) досяг $ 51,7 млрд. Про це свідчать дані аналітичної компанії MarketsandMarkets. Експерти не уточнили динаміку щодо 2018 року, але кажуть, що ринок є зростаючим і залишиться таким.

Очікується, що продажі витрати на програмно-визначенні мережі визначаються в глобальному масштабі і будуть збільшуватися на 25,5% щорічно, а до 2024 року вони досягнуть $ 160,8 млрд.

Хмарні технології докорінно змінюють основну модель витрат компаній, перетворюючи частину витрат на створення IT-інфраструктури з капітальних витрат в операційні і допомагають гнучко нарощувати додаткові ресурси або потужності на вимогу або в міру зростання бізнесу. Робочі столи співробітників стають віртуальними, перестаючи бути прив'язаними до чорних скриньок конкретних комп'ютерів. Набагато ефективніше вирішуються питання ліцензування програмного забезпечення та його своєчасного оновлення. Однак при цьому, хмарні технології і створюють певні проблеми, істотно ускладнюючи життя IT-фахівцям в тих випадках, коли потрібно зрозуміти, з чим пов'язана низька продуктивність сервісів і на чиєму боці виникла проблема.

РОЗДІЛ 2
РАКТИЧНІ АСПЕКТИ УПРАВЛІННЯ БЕЗПЕКОЮ ІНФОРМАЦІЙНИХ ПОТОКІВ МЕРЕЖІ IOT ЗА ДОПОМОГОЮ SDN

2.1 Проектування програмно-конфігурованої мережі на базі IoT

Software-defined Networking (SDN) це нова ідеологія побудови комп'ютерних мереж, в якій весь «інтелект», все управління мережею винесено на окрему апаратно-програмну базу (контролер), а все управління трафіком відбувається з використанням спеціальних протоколів, що оперують поняттям «потік» (flow) і керуючих їм [1]. На контролері встановлюється політика управління мережею на основі заданих правил і особливостей роботи спеціалізованих додатків.

За результатами експериментів було визначено, що за допомогою технології SDN можна підвищити ефективність мережевого обладнання, а також знизити витрати на експлуатацію мереж.

Основна мета – перетворити управління мережами з мистецтва в інженерію [2], підвищивши безпеку. Впровадження SDN має мати значний вплив на мережі дата-центрів, корпоративні мережі та ін.

Основні ідеї, закладені в SDN, полягають в наступному:

- поділ рівня передачі і рівня управління даними;
- єдиний, уніфікований, незалежний від постачальника інтерфейс між рівнем управління і рівнем передачі даних;
- логічно централізований рівень управління даними. Централізоване управління здійснюється за допомогою контролера з встановленою мережевою операційною системою і набором мережевих додатків, розгорнутих поверх її;
- віртуалізація фізичних ресурсів мережі.

OpenFlow є основною рушійною силою концепції мереж, що програмно-конфігуруються і найбільш широко застосовним стандартом їх побудови.

Головною особливістю мереж SDN є широкі можливості по віртуалізації, динамічному застосування мережевих політик і кращому

контролю над різними елементами мережі при малій вимогливості до обчислювальних ресурсів. Однак централізований контролер мережі вимагає підвищеної уваги з боку адміністратора для забезпечення безпеки і коректного функціонування всієї мережі. Елементи мережі, які зазнали атаки можуть бути використані для витоку інформації, атаки на інших користувачів або для виведення мережі з ладу.

Існуючі атаки на мережі SDN в тому чи іншому вигляді експлуатують основну їх особливість – централізований контролер. Їх можна класифікувати за типом загрози:

Атаки на топологію мережі:

- ARP Poisoning (підміна ARP пакетів);
- Fake topology (перебудова топології мережі);

Атаки на рівень управління даними:

- DoS контролера;
- TCAM exhaustion (переповнення пам'яті комутаторів);
- Switch blackhole (створення «чорної діри» в мережі);

Атака на рівень SDN.

Атаки на топологію мережі.

SDN контролер обробляє безліч пакетів (ARP, IGMP, LLDP і інші), які відправляються з комутаторів в рамках протоколу OpenFlow, щоб сконструювати своє уявлення про мережеву топологію. Ці повідомлення можна підмінити, що веде до появи можливості атакувати мережу.

ARP Poisoning

Хости, з яких проводиться атака, можуть підміняти інформацію про фізичні хости в мережі за допомогою підроблених ARP запитів. В результаті, контролер встановлює шкідливі правила для потоків в мережі і змінює їх напрямок для перехоплення трафіку, що призначався іншому хосту. Також, зловмисник може ініціювати випадкові потоки, щоб змусити контролер і комутатори створювати петлі і «чорні діри» в мережі або для здійснення IP

splicing атаки (атака, при якій встановилася сесія перехоплюється і зловмисник видає себе за вже авторизованого користувача підміною IP).

Fake topology

Один заражений хост намагається створити підроблену ланку в мережі, використовуючи лінійну топологію, що складається з трьох комутаторів X, Y і Z. Сервер A з'єднаний з комутатором X. Сервер відправляє шкідливий LLDP пакет, як ніби він прийшов від комутатора Z. В результаті атаки створюється підроблене односпрямоване ребро від Z до X в поданні контролера і відбувається перерахунок шляхів маршрутизації, що може порушити маршрутизацію і правильний напрямок потоків в мережі.

Атаки на рівень управління даними

Заражені хости і комутатори можуть провести DoS (Denial-of-service) атаку, завантаживши мережу трафіком до випадкових хостів, щоб вивести з ладу ресурси на вразливих комутаторах і / або сам SDN контролер, впливаючи на пересилку даних.

DoS контролер

Протокол OpenFlow вимагає від комутаторів відправляти пакети до контролера, якщо черги на вхід заповнені. Завантаживши мережу великим числом пакетів можна значно збільшити обчислювальне навантаження на контролер або навіть перервати його роботу.

TCAM exhaustion

Дані про маршрутизацію потоків в мережі зберігаються у швидкій асоціативній пам'яті TCAM.

Зловмисник може націлюватися на цю пам'ять комутатора, щоб атакувати інші хости.

Заражений хост відправляє безліч повідомлень в мережу і змушує контролер встановлювати велику кількість правил для потоків, витрачаючи TCAM. Згодом, нові правила не можуть запам'ятатися комутатором, поки старі не виконано. Якщо комутатор знаходиться в ключовій частині мережі, висока затримка або втрата пакетів гарантовані.

Switch blackhole

«Чорна діра» (blackhol e) це стан мережі, коли потоки різко обриваються і пакети не виходить доставити до пункту призначення. Заражений комутатор може скидати або перенаправляти пакети і в результаті потік не доходить. Це може значно порушити роботу мережі і бізнес-додатків, які не отримають потрібні дані.

Атаки на рівень SDN

Зловмисник вибирає метою своєї атаки API сервера. Сервер може використовувати будь-яку з безлічі мов програмування. Якщо вийде використовувати уразливість в API, а на контролері не буде ніякого захисту, тоді можна отримати повний контроль за мережею SDN через контролер. Наприклад, адміністратор забув поміняти пароль за замовчуванням. В такому випадку, зловмисник посилає пакети безпосередньо у керуючий інтерфейс контролера, отримує відомості про конфігурацію мережі або змінює її.

Надійність функціонування мережевої інфраструктури забезпечується шляхом використання алгоритмів резервування і відновлення зв'язку між мережевими вузлами і засобів підвищення надійності самих вузлів, в першу чергу комутаторів. Сьогодні всі серйозні технічні рішення вимагають модулів управління, які характеризуються надмірністю різних підсистем з можливістю їх швидкої заміни в «гарячому» режимі [15].

Таким чном, SDN для безпеки Інтернету речей у порівнянні з іншими підходами до побудови IoT використовує технологію резервування та відновлення зв’язку, також SDN взаємодіє з протоколами безпеки, основним з них є OpenFlow (OF), який передає повідомлення OF (Packet-In, Packet-Out, Flow-Add і т. д.)

При проектуванні мережі необхідно прагнути зменшити як ймовірність відмови, так і вплив відмови. Це непросте завдання, оскільки існує взаємний зв'язок між зниженням імовірності відмови і зниженням ступеня впливу відмови. Сучасні мережі – це мережі, що володіють величезною пропускною спроможністю і використовують як правило, оптичні лінії зв'язку. Тому

завдання забезпечення структурної надійності таких мереж є надзвичайно актуальним [16].

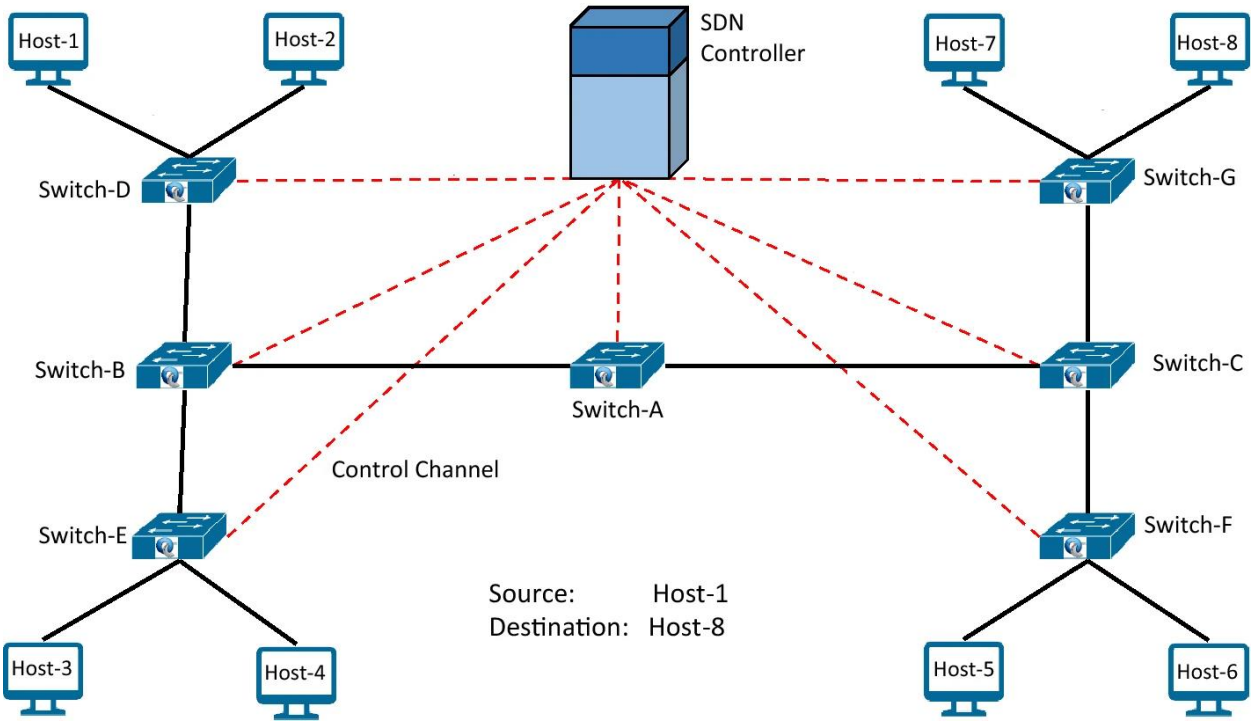


Рис. 2.1 Архітектура безпеки для мережевої інфраструктури Інтернету речей

На рисунку 2.1 представлена схема досліджуваної мережі. Контролер SDN - це саме технічно складний пристрій мережі, якщо відмовить контролер, то станеться обрив зв'язку із зовнішніми мережами. Для зв'язку із зовнішніми мережами використовуються маршрути через автономні системи BGP [41].

2.2 Модель управління безпекою інформаційних потоків мережі IoT

Між комутаторами і контролером для маршрутизації і цілей управління використовується протокол безпеки OpenFlow. У OpenFlow кожен комутатор містить таблицю потоків із записами потоків, доданими контролером на певний період часу для пересилки пакетів. Коли пакет прибуває в комутатор, він зіставляє заголовок пакета із записами потоку в таблиці потоків, щоб вжити відповідних заходів. Якщо немає відповідного запису, то заголовок

пакета інкапсулюється в повідомлення Packet-In і направляється до контролера для відповідної дії. Контролер додає запис потоку в комутатор, відправляючи повідомлення Flow-Add, що відображає відповідну дію [6]. В наші дні підтримка OpenFlow надається в мережевих комутаторах такими великими постачальниками, як Juniper, HP і Cisco

Резервування і відновлення є двома основними підходами, що забезпечують структурну надійність мереж при виході з ладу вузлів і ліній зв'язку. Основними вимогами до методів забезпечення надійності є:

- економія пропускної здатності;
- обмеження на комп'ютерні ресурси;
- швидкість заміщення;
- складність передбачуваних методів;
- масштабованість [17].

Зауважимо, що завдання оптимізації будь-якого з показників при наявності обмежень є в більшості випадків складним завданням. Для її вирішення можуть використовуватися різні методи. А саме, метод невизначених множників Лагранжа, методи лінійного та нелінійного цілочисельного лінійного програмування та ін. Однак найчастіше для вирішення поставленого завдання використовують евристичні методи.

Для підвищення надійності систем та елементів використовують резервування, що полягає в застосуванні того чи іншого виду надмірності. Види резервування діляться на 4 типи: структурне, інформаційне, тимчасове і програмне. В інформаційному резервуванні використовують надмірну інформацію. Тимчасове резервування - застосування надмірного часу. Програмне резервування - надлишкових програм [18]. Всі ці види резервування в системі використовуються в цілому або окремо.

Види резервування за схемою включення елементів діляться на постійне, роздільне, резервування із заміщенням і на ковзне резервування. При постійному резервуванні резервні елементи працюють разом з основними і є найбільш надійними методами з вище перерахованих (рисю.2.2). При

постійному резервуванні при відмові не потрібні особливі конструкції для включення резервних елементів в роботу.

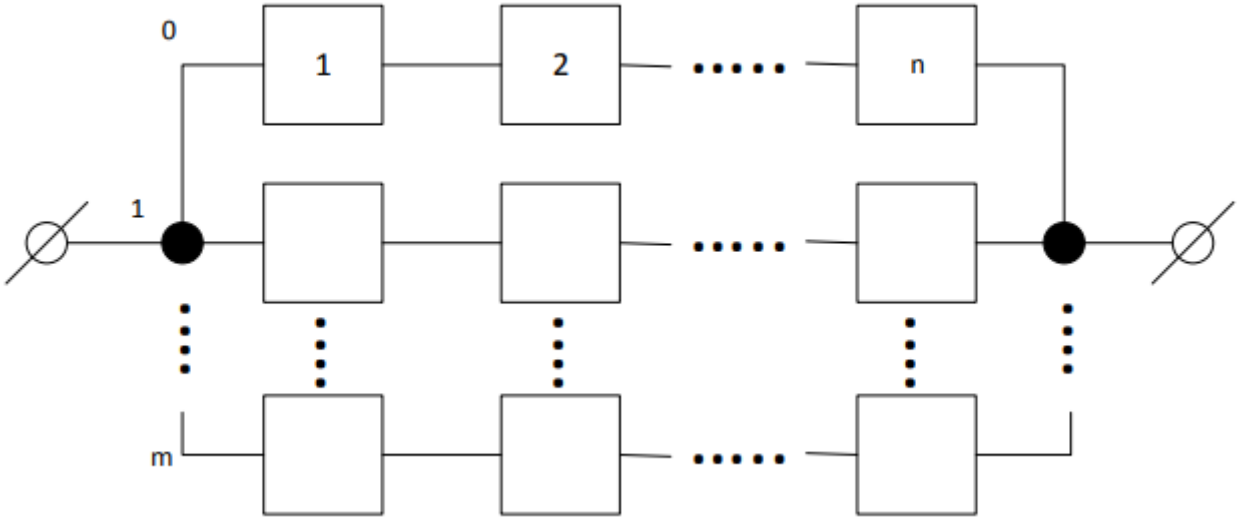


Рис. 2.2 Загальне резервування з постійним резервом

Роздільним резервуванням називається метод підвищення надійності при якому резервуються окремо елементи системи (рис.2.3).

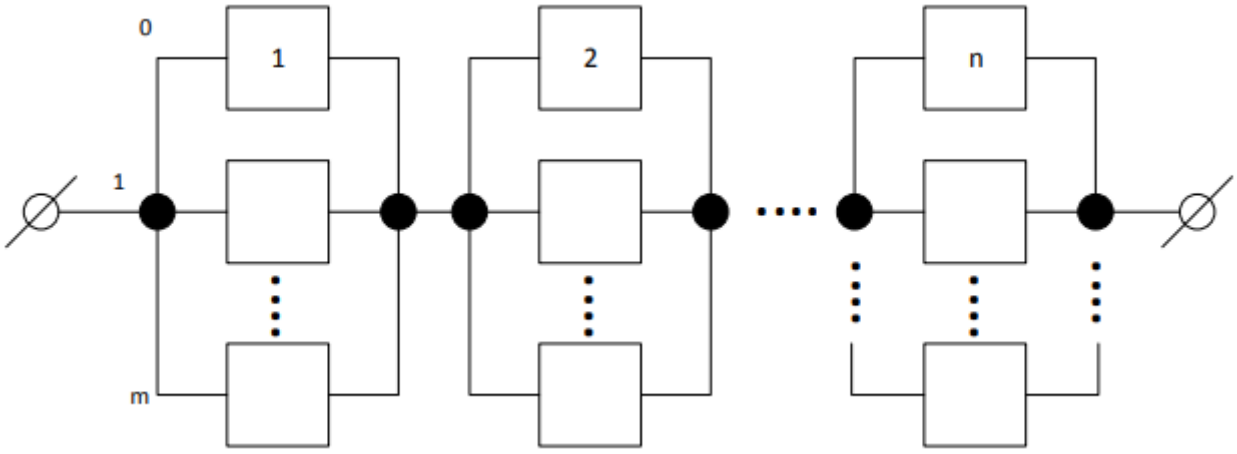
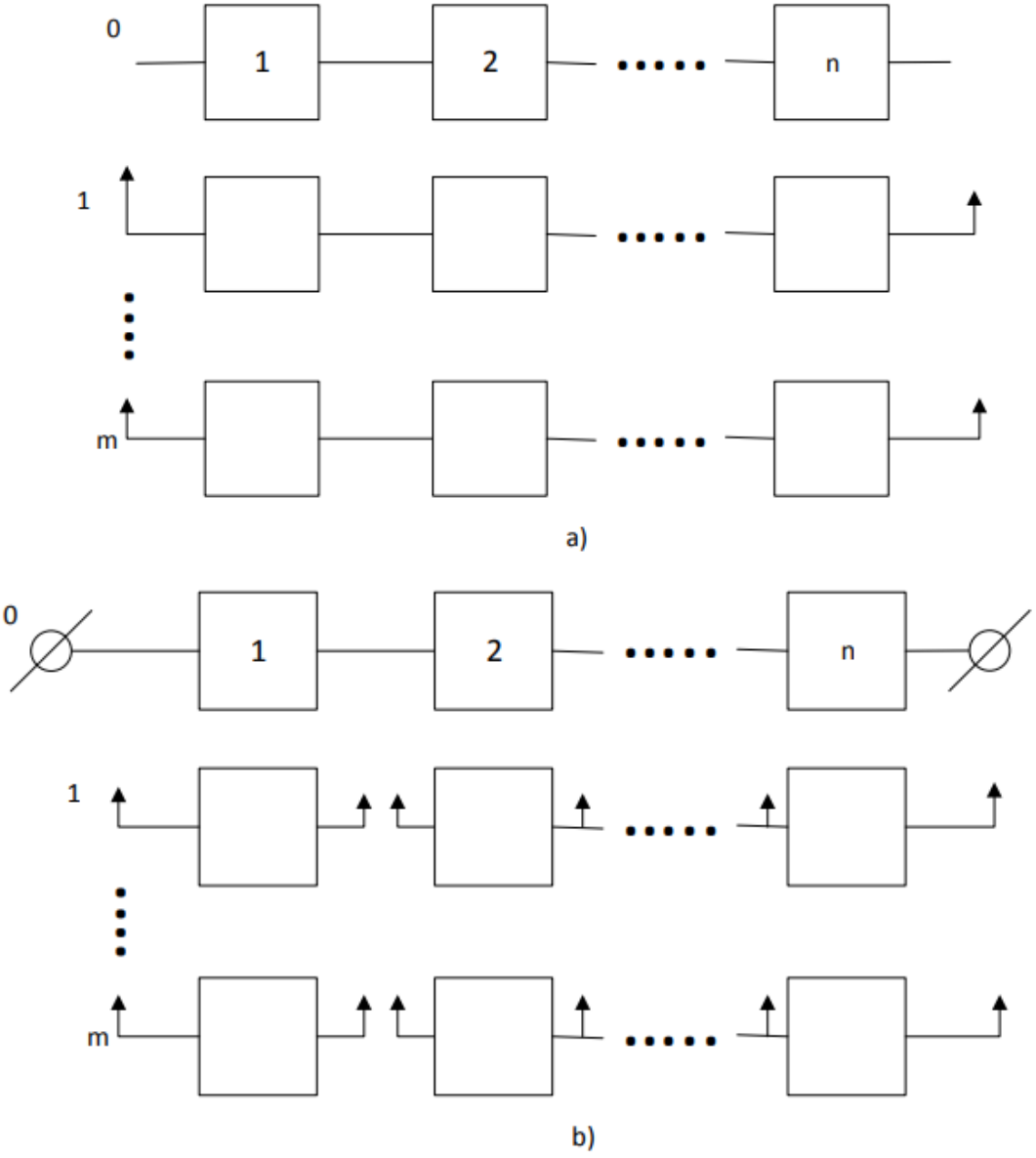


Рис. 2.3 Роздільне резервування з постійним резервом

Головним параметром резервування є його кратність (ступінь надмірності). Під кратністю резервування розуміється відношення числа резервних елементів до числа елементів, що резервуються (основних). Резервування заміщенням – це резервування, при якому функції основної

системи передаються резервному тільки після відмови основної системи (рис.2.4 а,б). При застосуванні резервування заміщенням потрібні контролюючі та перемикаючі пристрої для виявлення факту відмови основного елемента і перемикання його з основного на резервний [19].



а) - загальне резервування; b) - роздільне резервування

Рис. 2.4 Резервування за включеним заміщенням резерву

При ковзному резервуванні група основних елементів резервується одним або декількома резервними елементами, існує можливість змінити елемент, що відмовив в будь-який з груп основної системи (рис. 2.5).

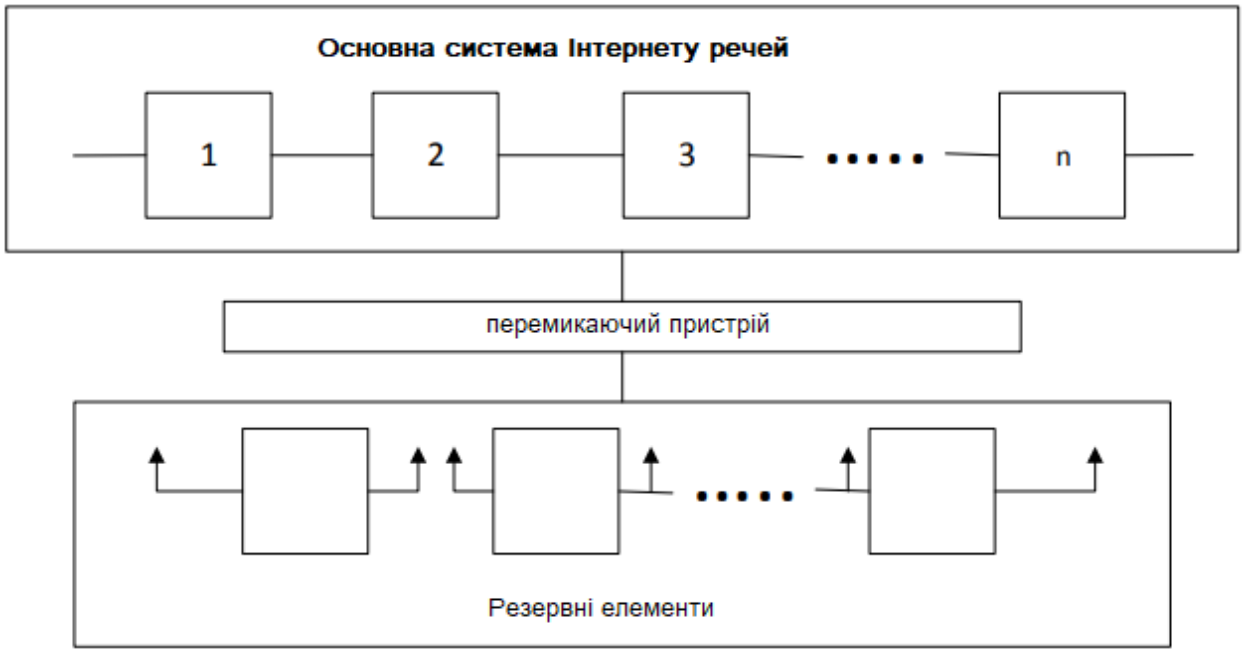


Рис. 2.5 Схема змінного резервування

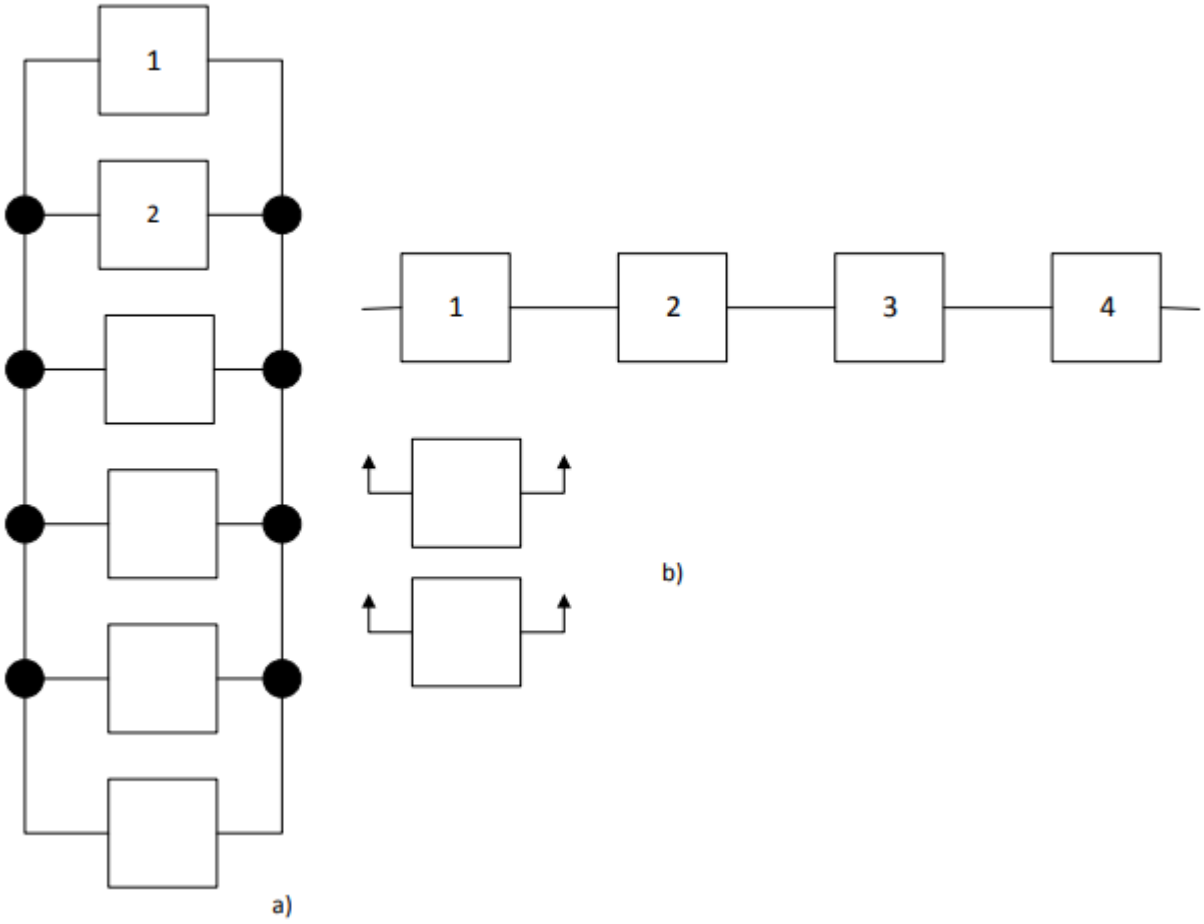
Резервуванням називають метод підвищення надійності об'єкта шляхом введення надмірності. Завдання включення надмірності – забезпечення нормального функціонування системи після виникнення відмов в її елементах. Структурне резервування (або апаратне) передбачає використання надлишкових елементів систем. Суть такого виду резервування полягає в тому, що в мінімально необхідний варіант системи, елементи якої називають основними, вводяться додаткові елементи, вузли, пристрої або навіть замість однієї системи передбачається використання декількох ідентичних систем [18].

Залежно від режиму роботи розрізняють:

- навантажений резерв – резервний елемент знаходиться в тому режимі роботи, що й основний. При цьому приймається, що характеристики надійності резервних елементів в період їх перебування в якості резервних і в період використання замість основних після відмови останніх, залишаються незмінними;
- полегшений резерв – резервний елемент знаходиться в менш навантаженому режимі, ніж основний. Приймається, що

характеристики надійності резервних елементів в період їх перебування в якості резервних вище, ніж в період їх використання замість основних після відмови останніх.

Розрізняють резервування з цілою і дробовою кратністю. Для їх відмінності на схемі вказують кратність резервування m (рис. 2.6).



a) постійне резервування з кратністю (m = 4/2);

b) роздільне резервування з кратністю (m = 2/4)

Рис. 2.6 Резервування з дробовою кратністю

Для резервування систем, що складаються з рівних елементів, можна застосовувати незначне число резервних елементів замість будь-яких, що відмовили основних елементів (ковзне резервування). Ненавантажений резерв - резервний елемент, який майже не несе навантаження. Такий резервний елемент, перебуваючи в резерві, відмовляти не повинен, тобто володіє в цей період досконалою надійністю. У період же застосування цього елемента

замість основного після відмови останнього надійність стає рівноправною надійністю основного.

Окремим випадком резервування з дробовою кратністю є мажоритарне резервування, яке широко використовується в пристроях дискретної дії (рис.2.7). При мажоритарному резервуванні замість одного елемента (каналу) приєднується три ідентичних елемента, виходи, яких подаються на мажоритарний орган М (елемент голосування). Якщо всі елементи цієї резервної групи справні, то на вхід М надходять три однакових сигнали і такий же сигнал надходить у зовнішній ланцюг з виходу М.

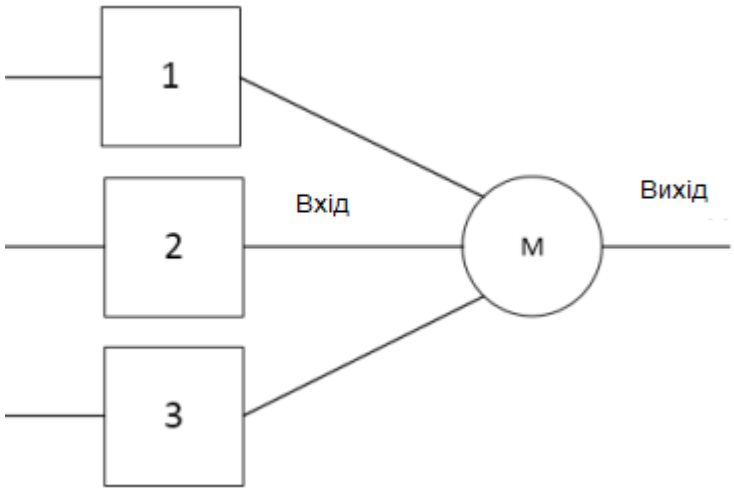


Рис. 2.7 Мажоритарне резервування (вибір по більшості)

Якщо один з трьох резервних елементів відмовив, то на вхід М надходять два однакових сигнали (істинних) і один сигнал помилковий. На виході М буде сигнал, що співпадає з більшістю сигналів на його вході, тобто мажоритарний орган, здійснює операцію голосування або вибору за більшістю. Таким чином, умовою безвідмовної роботи системи при мажоритарному резервуванні є безвідмовна робота будь-яких двох елементів з трьох і мажоритарної системи протягом заданого часу [20]. Комбінований резерв – на рис. 2.8 показана резервована група, що з'єднує переваги навантаженого резерву (безперервність роботи) і не навантаженого резерву (забезпечення великого виграшу в надійності). В даному випадку два елементи

утворюють дублюючу групу (навантажений резерв), а третій знаходиться у ненавантаженому резерві. Такий резерв називають комбінованим.

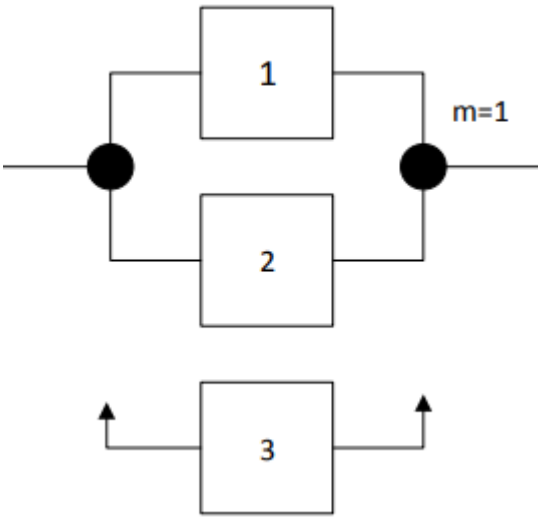


Рис. 2.8 Комбінований резерв

У пристроях керуючого призначення можуть бути застосовані всі види структурного резервування (рис. 2.9).

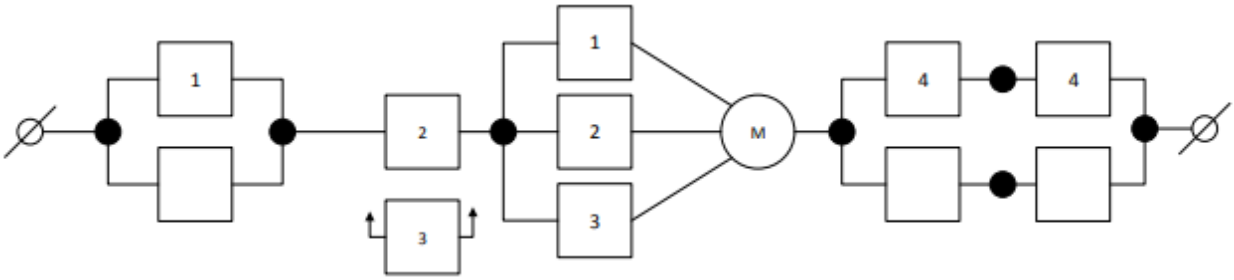


Рис. 2.9 Розрахунково-логічна схема структурного резервування

Теоретично впровадженням надмірності в структуру системи і вибором оптимальних режимів можна сформувати надійну систему. Розглядаючи всі види резервування, слід зробити практичний висновок: забезпечити високу надійність шляхом загального навантаженого резерву не представляється можливим з економічних міркувань. Граничний ефект дає по елементне резервування [21].

Порівнюючи між собою види резервування з навантаженим і ненавантаженим резервом, можна помітити, що при однакових умовах система з ненавантаженим резервом надійніше системи з навантаженим резервом.

Надійність систем безпосередньо залежить від методів резервування між мережевими пристроями. Комплекс технічного обладнання та комунікаційних ліній, призначених для формування спеціалізованої передачі джерел інформації називають як тракт інформаційної передачі.

Для визначення ступеня захисту, необхідної для даної ділянки мережі, необхідно враховувати ймовірність відмови ділянки мережі і передбачувані впливи на трафік (в поняттях часу відновлення, ймовірно втрати пакетів) [22]. Значення ймовірності відмови області захисту можна визначити на підставі доступної інформації про характер відмов, що що відбуваються.

Початкове значення ймовірності відмови може бути уточнено на основі фактичної статистики відмов. Якщо ймовірність відмови відома, необхідно вивчити, як відмова впливає на трафік в мережі, тобто, визначити «ступінь впливу відмови». Критичним аспектом для оцінки впливу відмови є якість обслуговування (QoS) трафіку, яка визначається двома компонентами: часом відновлення і кількістю втрачених пакетів. Час відновлення ТБ визначається циклом відновлення шляху.

Зауважимо, що цей цикл можна задати такими складовими:

1) часом виявлення відмови T1;

2) часом утримання (в разі необхідності) T2;

3) часом повідомлення (тобто посилки повідомлення вузлу, відповідального за перемикання) T3;

4) часом для резервування маршруту і сигналізації T4;

5) часом для перемикання трафіку T5 з активного шляху на резервний шлях.

Кількість втрачених пакетів NПП пропорційно часу відновлення ТБ і швидкості передачі пакетів R, тобто NПП = RTB.

Скорочення часу виявлення відмови і часу перемикання залежить від використовуваної технології відновлення. Крім того, час встановлення резервних шляхів (при виявленні відмови) залежить від методу маршрутизації і використовуваних методів сигналізації. Скорочення часу повідомлення $T_З$ - ймовірно, основний аспект при проектуванні методів захисту для мережі. Час повідомлення залежить від часу поширення між вузлами сигналу про відмову $T_р$ і від відстані $D\ (i, a)$, яка може бути визначена як кількість ділянок мережі (ребер) між вузлом, який виявив відмову (вузол а), і вузлом, відповідальним за перемикання (вузол і) [14].

$$T_{УВ} = T_Р \cdot D\ (i, a) \qquad (2.1)$$

Якість обслуговування також важливий критерій для клієнтів, і відповідно, для постачальників послуг. Існуючі призначені для користувача угоди про рівень послуг, що надаються (SLA - Service Level Agreement) дозволяють користувачам пред'являти гарантійні претензії при невиконанні договору постачальником або не якісне надання послуг. Гарантійні претензії впливають на прибуток, а також обсяги продажів через незадоволеність клієнтів. Щоб мінімізувати кількість претензій, виробники постійно підвищують надійність своїх продуктів.

Хоча підвищення надійності сприяє зниженню витрат на відмову, відбувається збільшення витрат на профілактику і оцінку (Preventive and Appraisal Costs - PAC). Витрати на відмову і на профілактику і оцінку формують функцію загальній вартості якості (Total Quality Cost - TQC) [23].

Рис. 2.10 Залежність функцій оцінок витрат від рівня якості

У міру підвищення надійності функція ΔPAC збільшується, в той час як функція ΔFC зменшується. Функція TQC має свій локальний мінімум на перетині оптимальної вартості якості (OQC - Optimum Quality Cost) і оптимального рівня якості (OQL - Optimum Quality Level), тобто в точці де ΔPAC = ΔFC. Цей момент є оптимальним рішенням для постачальника послуг, але не обов'язково оптимальним для клієнта. З іншого боку підхід заснований на повному задоволенні клієнта в аспекті надійності, радує користувача, але може завдати серйозної шкоди бізнес-стратегії постачальника, тобто позначитися на прибутку [24].

Фактично підвищення якості призводить до більш високої вартості, але не обов'язково збільшує функцію загальної вартості якості або вартість надання послуг.

Іншою стороною питання надання гарантованого рівня якості, а відповідно необхідної надійності є те факт, що для різних категорій користувачів існують різні угоди (SLA) і, отже, їм потрібен різний рівень якості послуг, що надаються.

Йдеться про звичайних пересічних користувачів, і про користувачів бізнес-сегмента [25]. У більшості випадків якщо постачальник послуг не

виконав свої зобов'язання належним чином, то звичайний користувач може скласти претензію і на цьому все обмежиться. Якщо таких претензій будуть одиниці, то постачальник не буде намагатися змінити свою політику в області надійності, але якщо претензії будуть надходити у величезній кількості, то постачальнику доведеться або знизити вартість послуг, що надаються, або збільшити свої витрати на підвищення надійності, тим самим зменшивши кількість претензій.

Для клієнтів бізнес-сегменту ситуація видається інакше, якщо постачальник не виконав свої зобов'язання, то клієнту відшкодовується компенсація за не надання необхідної якості. Постачальник послуг може провести аналіз своїх витрат, і якщо витрати на виплати компенсацій будуть перевищувати витрати на підвищення надійності, то розумніше буде підвищити рівень якості послуг, що надаються, але якщо станеться все навпаки, то постачальник не вдаватиметься до подібних заходів [26].

Узагальнена характеристика методів захисту від відмов представлена в таблиці 2.1.

Таблиця 2.1

Узагальнена характеристика методів захисту від відмов

Методи захисту		
Захисне перемикання (резервування)	Відновлення (перемаршрутизація)	
Виділення ресурсів		
Попереднє	За вимоги	
Використання ресурсів		
Виділені	Загальні	Другорядного трафіку
Створення шляху		
Попереднє	У відповідністю з якістю	За вимогою
Масштаб захисту		
Глобальна (шлях)	Глобальна (шлях)	Глобальна (шлях)
Захисне перемикання		
Резервування	Відновлення	
Автоматичне (внутрішній сигнал)	Автоматичне (внутрішній сигнал)	Автоматичне (внутрішній сигнал)

2.3 Алгоритм управління безпекою інформаційних потоків мережі IoT за допомогою SDN

У роботах по дослідженню та забезпечення надійності велике місце займають статистичні методи досліджень і імовірнісні оцінки надійності. Це обумовлено тим, що події і величини, які використовуються в теорії надійності, носять, як правило, випадковий характер. Відмови об'єктів викликаються великою кількістю причин, зв'язок між якими встановити не можливо, тому відмови виробів належать до категорії випадкових подій. Час до виникнення відмови може набувати різних значень в межах певної області можливих значень і належить до категорії випадкових величин [31].

Розрахунки надійності мають на меті отримання якісних значень показників надійності досліджуваного об'єкта. Ці розрахунки стали обов'язковим елементом на всіх етапах розробки, створення і використання технічних систем.

При аналізі надійності системи основні труднощі представляє складання структурної схеми розрахунку і аналітичних (розрахункових) формул.

Існуючі в даний час розрахункові формули отримані при великому числі обмежень (припущень). Найбільш часто такими обмеженнями є:

- обов'язковість експоненціального розподілу часу до відмови об'єкта і часу відновлення його працездатності;
- досліджувані процеси – марківські, досліджувані потоки подій – найпростіші;
- при розрахунках враховуються тільки середні значення показників надійності [32].

Найпростіший потік знаходить широке застосування в теорії надійності з урахуванням наступних факторів:

- є гранична теорема, згідно з якою сума більшого числа незалежних потоків з будь-якими законами розподілу наближається до найпростішого потоку з ростом числа доданків потоків;

– практика дослідження потоків відмов, потоків відновлень і інших потоків, що мають місце при дослідженні надійності, підтверджує обґрунтованість припущень про широку поширеність найпростіших потоків.

Вибір моделі надійності – складна науково-технічна задача. Вона може бути вирішена методами математичної статистики, якщо є великий статистичний матеріал про відмови досліджуваної системи. З огляду на новизну SDN та її компонентів, статистичних даних недостатньо для використання методів математичної статистики. У нашому випадку при виборі моделі керуються результатами випробувань і фізичними міркуваннями.

У разі наближених оцінок часто вибирається експоненціальна модель як найбільш зручна з точки зору аналітичних перетворень. Цю модель рекомендується використовувати при виконанні розрахунків надійності при відсутності інших вихідних даних, крім інтенсивностей відмов.

Для опису імовірнісного процесу (тому що функціонування будь-якої технічної системи є реалізацією імовірнісних процесів) необхідно вказати тип процесу і його числові характеристики. Найбільш часто для опису процесів, що відбуваються в системах, використовується марківський процес [33]

Необхідною умовою для марковського процесу є експоненціальний розподіл часу роботи до відмови і часу відновлення працездатності. Найважливіша числова характеристика такого процесу - ймовірність переходу об'єкта в той чи інший стан за заданий проміжок часу. Знаючи це, можна визначити ймовірності кожного з можливих станів об'єкта.

Для відновлення в мережі SDN протокол OpenFlow організовує оригінальний спосіб відновлення [34]. Для відновлення використовується наступний алгоритм. Після виявлення відмови контролером мережі ця відмова фіксується і складається список трактів LSP порушених виниклою відмовою. Для кожної нової відмови на моделі мережі розраховується обхідний шлях, який діє в контролері.

Проводиться відновлення за алгоритмом CSP, за результатами роботи якого протокол OpenFlow коригує таблиці комутації відповідно з розрахованими маршрутами трактів [35].

Для боротьби з втратами пакетів, як зазначалося вище, використовується алгоритм перемаршрутизації. При перемаршрутизації необхідно організувати новий резервний шлях, але не перезавантажити ланки цієї нової колії не більш як на 70%. Вибір даного кордону в області 70% пояснюється тим, що зростає затримка при збільшенні ступеня завантаженості каналу.

Різкий стрибок затримки з'являється після рівня завантаження каналу в 70% (рис.2.12). Тому даний рівень завантаженості обраний в якості граничної межі.

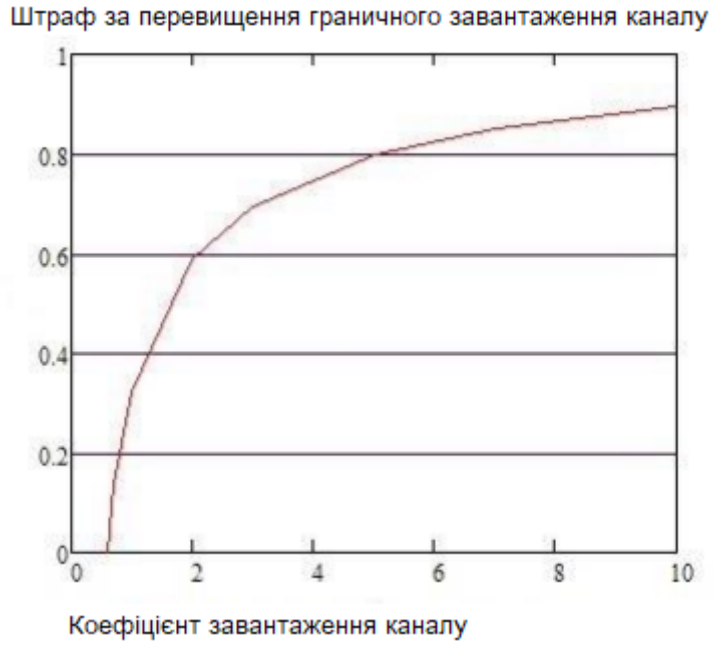


Рис. 2.12 Графік залежності затримки в каналі від ступеня його завантаженості

У більшості випадків рішення задачі перемаршрутизації зводиться до проблеми CSP (Constrained Shortest Path) - проблеми побудови найкоротших шляхів з урахуванням обмежень, що вводяться. У цьому методі відшукуються мінімальні значення функції вартості всіх шляхів, яка визначається у вигляді

суми вартостей всіх сформованих на мережі шляхів f_c (r) при виконанні обмежень по сумарній затримці f_D (r).

Маршрутизація в методі CSP еквівалентна тому, що найкоротший шлях знаходиться майже виключно за кількістю стрибків (h_{op}).

Особливість методу CSP є швидка збіжність і висока швидкість, що дозволяє використовувати його для вирішення завдань в реальному часі, тобто при експлуатації мережі [36].

Метод CSP зважаючи на його високу швидкість може використовуватися як для визначення обхідних шляхів в реальному часі після виявлення відмови у час експлуатації мережі, так і для попереднього визначення обхідних шляхів при проектуванні мережі. При повному розрахунку надійності необхідно також оцінити надійність управління в мережах SDN, яка виробляється за допомогою контролерів [37].

Контролер в мережі SDN є ключовим елементом, оскільки він виконує функції управління елементами мережевої інфраструктури і потоками даних в мережі. Характеристики надійності мережі SDN залежать безпосередньо від відповідних характеристик надійності контролера.

У даній роботі розглядаються лише методи (механізми) відновлення при відмовах на мережі ПКС і не розглядається сам моніторинг мережі. Можна лише відзначити що моніторинг буде проводиться за допомогою періодичної організації в площині даних сеансів протоколу BFD (Bidirectional Forwarding Detection). Даний протокол практично не впливає на продуктивність, тому забезпечує швидку збіжність. Робота двостороннього протоколу BFD основа на те, що пов'язані пристрої генерують BFD-пакети, а також відповідають на BFD-пакети від сусіднього пристрою (пакети-відповіді містять набір ознак, однозначно характеризують даний пакет [38]). Таким чином гарантується що інформаційний потік не буде спрямований по пошкодженій ділянці мережі.

На додаток до дослідницької роботи можна повідомити про інший напрямку досліджень в області підвищення надійності SDN. Для широкомасштабного розгортання SDN часто потрібно кілька контролерів, а

розміщення цих контролерів стає важливим завданням. В роботах [39] розглядаються питання розміщення контролерів з метою максимізації надійності мереж управління. Надається нова метрика, звана відсотком втрат в тракті управління, щоб охарактеризувати надійність мереж управління SDN. Формулюється проблема розміщення контролера, пропонується кілька алгоритмів розміщення, які допомагають вирішити цю проблему. Завдяки моделюванню з величезною кількістю топологій, наочно демонструється як кількість контролерів і їх розміщення впливають на надійність мереж управління. Крім того авторами дослідження робиться висновок, про те, що при правильному (вдалому) розташуванні контролерів надійність мереж управління значно поліпшується без впровадження неприйнятних затримок між комутаторами і контролерами.

Висновки

У рамках другого розділу розкрито принципи управління безпекою мережі. Наведено модель управління безпекою інформаційних потоків мережі IoT та запропоновано алгоритм управління безпекою інформаційних потоків мережі IoT за допомогою SDN.

Безпека грає ключову роль в подальшій міграції мережевих сервісів в «хмари» і для подальшого розвитку SDN. Список областей, де поки не варто використовувати SDN досить великий, проте з часом технологія буде вдосконалена і для неї будуть розроблені надійні системи управління. Разом з тим, слід зазначити, що ЦОД повинні самі забезпечувати захист обчислювальної архітектури і цілісність SDN, а програмний контролер, керуючий мережею, є частиною загальної керуючої системи всього ЦОД. Перевагою технології SDN та її слабким місцем є централізоване управління мережею і маршрутизацією в ній. Обдуривши контролер або отримавши над ним контроль можна в тій чи іншій мірі порушити роботу всієї мережі.

РОЗДІЛ 3
ЕФЕКТИВНІСТЬ УПРАВЛІННЯ БЕЗПЕКОЮ ІНФОРМАЦІЙНИХ ПОТОКІВ МЕРЕЖІ ІОТ ЗА ДОПОМОГОЮ SDN

3.1 Методологія визначення ефективності управління безпекою інформаційних потоків мережі IoT за допомогою SDN

Аналіз надійності телекомунікаційних систем проводиться за допомогою аналітичних методів, а також імітаційного і статичного моделювання.

Основою аналітичних методів є теорія випадкових процесів (з нашого завдання - марковських). За допомогою однорідних марковських процесів з кінцевим числом станів описується система при обмеженнях. Час знаходження в одному стані розподілено по показовому закону. Даний розподіл можна використовувати лише тоді, коли потоки є найпростішими, тобто мають властивості ординарності, стаціонарності і відсутність післядії.

Випадкові процеси зустрічаються в теорії надійності виходять за межі марковських процесів. Якщо відмовитися від використання експоненціально відмов і відновлень, то це призведе до труднощів складання інтегродиференціальних рівнянь [40].

При дослідженні впливу резервування на надійність мережі, дослідник стикається з багатьма труднощами, пов'язаними зі складністю технічної системи і великим числом станів для її функціонування, що призводить до необхідності вирішення систем рівнянь великих розмірностей.

У справжніх методах розрахунку надійності приймається допущення, що відмови елементів незалежні, і система потрапляє в стан відмови при відмові певного числа елементів.

Предметом дослідження є мережа підприємства, побудована за принципами технології SDN, де використовуються комутатори з малим функціоналом, а всі головні завдання управління, маршрутизації та іншого виконує контролер SDN.

Для дослідження впливу резервування SDN контролера, вводимо допущення при обчисленнях:

– при відмові одного з маршрутів, смуга пропускання, що залишилася достатня для задоволення підприємства;

– розглянута мережа вважається непрацездатною при відмові контролера SDN, а також при відмові всіх комутаторів;

– при роботі мережі, в один момент часу може відмовити тільки один сервер;

– час відновлення контролера набагато більше часу відновлення комутатора, тому відновлення комутатора відбувається непомітно при одночасному відновленні контролера.

Для даної мережі складемо список станів:

1) відмови відсутні;

2) відмова одного комутатора;

3) відмова двох комутаторів;

4) відновлення комутатора при робочому сервері;

5) відновлення двох комутаторів при робочому сервері;

6) відмова сервера;

7) відмова комутатора і сервера;

8) відмова сервера і двох комутаторів;

9) відновлення контролера;

10) контролер з кластера серверів непрацездатний.

Для захисту SDN від DoS-атак протягом останніх кількох років були запропоновані різні методи. Більшість методів блокують підозрілий трафік, встановлюючи правила для відкидання всіх пакетів, в той час як інші зменшують наслідки атаки шляхом балансування навантаження, агрегації потоків, планування пріоритетів або використання значень довіри. Дуже складно судити за такий короткий час і з високою точністю, чи є дані, відправлені вузлом, законними або підробленими; отже, є ймовірність втрати даних, відправлених легітимним вузлом. Отже, потрібні більш надійні методи,

спрямовані на запобігання втрати законних даних; проте вони також можуть страждати від таких проблем, як потреба в додатковому обладнанні, модифікація комутатора, втрата детальної інформації, додаткова затримка у встановленні маршруту, додаткові пакети управління або стану гонки і т. д.

У даній дипломній роботі пропонується модель установки з паралельним потоком, щоб зменшити наслідки DoS-атак в SDN без шкоди для детального контролю мережевого трафіку.

Пропонована модель долає такі проблеми, як:

- додаткові вимоги до обладнання,
- модифікація комутатора,
- додаткова затримка у встановленні маршруту,
- втрата інформації і додаткові пакети управління.

Працездатність запропонованої моделі оцінюється шляхом порівняння її з базовим контролером SDN. Результати моделювання показують, що пропонована модель збільшує обслуговуючу здатність існуючої інфраструктури SDN за рахунок зменшення часу відгуку, зменшення обробки ЦП і зменшення трафіку в каналі управління. Крім того, пропоновану модель можна використовувати з будь-яким існуючим підходом до пом'якшення наслідків, щоб зробити її більш ефективною.

SDN контролер, який є централізованим органом, зберігає і підтримує оновлену інформацію про всю мережі. Процес маршрутизації також управляється контролером за допомогою повідомлень OF, таких як Packet-In, Packet-Out, Flow-Add і т. Д [2]. Комутатори містять таблиці потоків для зберігання правил потоку протягом обмеженого часу і пересилання даних відповідно до цих правил. Контролер зберігає топологію мережі в своїй базі даних, щоб забезпечити ефективну та своєчасну маршрутизацію до підключених вузлів. Додатки / модулі маршрутизації в добре відомих контролерах SDN з відкритим вихідним кодом, таких як Floodlight (проштовхувач ланцюгів) [13], ONOS (fwd) [14], Ryu (simple_switch, simple_switch_12, simple_switch_13) [15] і POX (L2_learning), L3_learning) [16]

і т. д., встановіть правила потоку на комутаторах OF лінійним чином, де кожен комутатор на шляху між джерелом і пунктом призначення відправляє повідомлення Packet-In в сторону контролера. Мережева діаграма, показана на рис. 3.1, пояснює процес маршрутизації між джерелом (Host-1) і одержувачем (Host-8) в SDN.

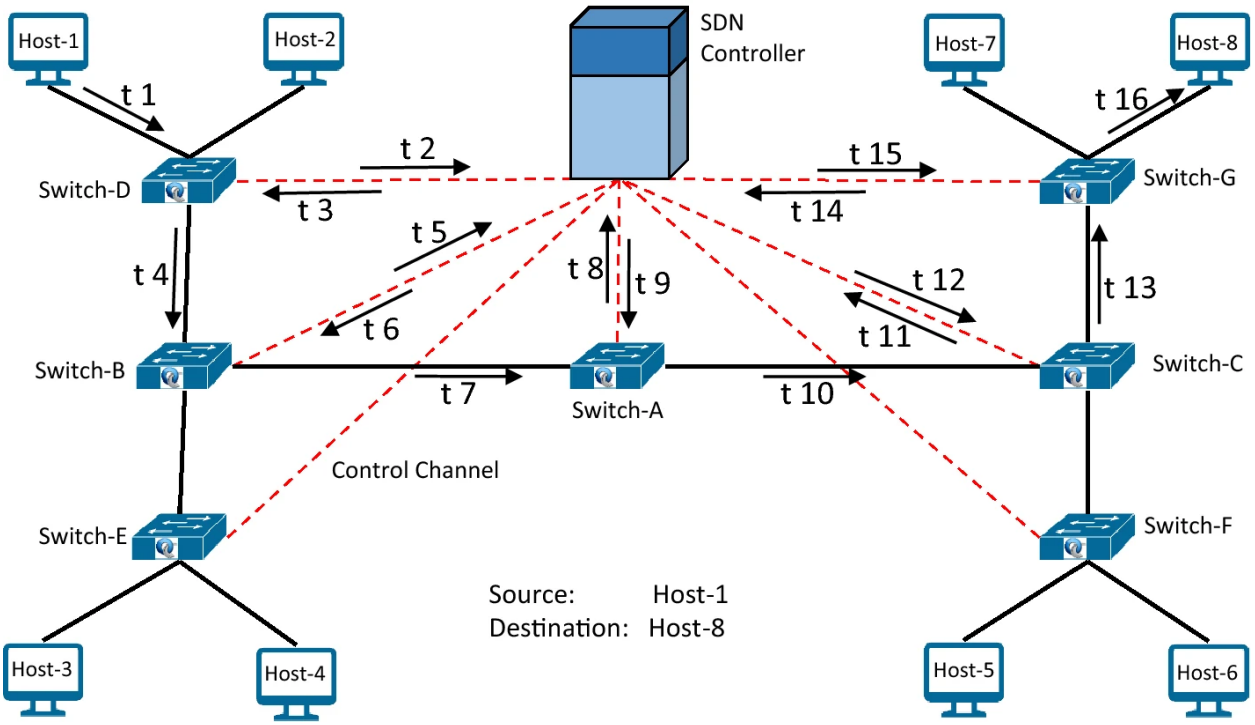


Рис. 3.1 Мережева діаграма. Процес маршрутизації SDN

На рис. 3.1 суцільні лінії представляють зв'язок між комутаторами і хостами, а пунктирні лінії представляють зв'язок між контролером і комутаторами. У термінології SDN зв'язок між контролером і комутатором називається каналом управління. Стрілки являють собою переміщення даних від вихідного вузла (Host-1) до цільового вузла (Host-8) в різні проміжки часу. У момент t1 вихідний вузол відправляє пакет даних комутатору-D, який виконує пошук в своїй таблиці потоків для пересилання даних. Відсутність таблиці відбувається, коли в таблиці потоків не знайдено жодного підходящого правила потоку, в результаті чого комутатор генерує повідомлення Packet-In і відправляє його контролеру через канал управління в

момент часу t2. Після отримання повідомлення Packet-In контролер переглядає свою таблицю маршрутизації, щоб знайти маршрут до місця призначення, і відправляє повідомлення Flow-Add, що містить інструкції з пересилання даних назад в Switch-D в момент t3. Якщо в таблиці маршрутизації контролера немає маршруту до пункту призначення (тобто вузол призначення ще не зв'язувався з будь-яким іншим вузлом в мережі), то контролер відправляє повідомлення Packet-Out на Switch-D з проханням надіслати електронний лист. Після отримання повідомлення Flow-Add від контролера Switch-D пересилає дані Switch-B в момент t4. Комутатор B також відправляє повідомлення Packet-In, отримує повідомлення Flow-Add і пересилає дані комутатора A в момент часу t5, t6 і t7 відповідно. Аналогічним чином Switch-A, Switch-C і Switch-G запитують у контролера шлях протягом часу від t8 до t15, і, нарешті, Switch-G передає дані в пункт призначення в момент t16.

Тепер, якщо цільовий вузол також хоче спілкуватися з вихідним вузлом, всі ці кроки будуть повторюватися в зворотному порядку. Крім того, якщо ці два вузли знову обмінюються даними один з одним після певного періоду часу, щоб зберегти правила потоку в таблиці потоків, то всі вищезгадані кроки будуть повторюватися знову.

Згідно рис. 3.1, якщо є п'ять перемикачів між джерелом і одержувачем, то контролеру буде відправлено не менше п'яти повідомлень Packet-In; отже, будуть встановлені п'ять правил потоку для передачі даних до місця призначення.

У парадигмі SDN зловмисникові легко запустити DoS-атаку шляхом лавинної розсилки пакетів з випадковими адресатами таким чином, щоб комутатор OF пересилав кожен пакет контролера, щоб отримати нове правило потоку. Ця атака торкнеться різних компонентів інфраструктури SDN, споживаючи їх ресурси, такі як пам'ять комутатора, пропускна здатність каналу управління і обчислювальна потужність контролера. Це надмірне використання ресурсів може призвести до низької пропускної здатності, високої затримки або законному відкиданню пакетів. У SDN атака DoS не

обов'язково робить недоступною всю мережу або деякі її сегменти; скоріше це може перевантажити мережеві ресурси таким чином, що дані не будуть доставлені належним чином [7].

Через наявність різних форм і здатності атакувати різні компоненти інфраструктури SDN, DoS-атаки дуже важко виявити і пом'якшити. Зловмисник може розсилати пакети на різні вузли в мережі, щоб використовувати ресурси комутатора і контролера (пам'ять і обчислювальну потужність), або може відправляти пакети великого розміру на різні вузли в мережі, щоб використовувати їх пропускну здатність. У законного користувача також може бути потреба в багаторазовому скануванні всієї мережі або відправці великої кількості даних на різні вузли. Отже, в стратегії пом'якшення наслідків складно відрізнити зловмисника від законного користувача. Більш того, підхід до пом'якшення наслідків не повинен мати компромісу за рахунок точних умов потоку (MAC-адреса джерела і призначення, IP-адреса, номери портів і т. д.).

3.2 Ефективність управління безпекою інформаційних потоків мережі IoT за допомогою SDN

Підхід до зниження DoS-атак можна розділити на дві категорії. Перша категорія містить підходи, які блокують шкідливий трафік, встановлюючи правила для відкидання всіх пакетів зі шкідливих вузлів. До другої категорії відносяться підходи, що не скидають шкідливий трафік. Ці підходи зменшують вплив DoS-атак за рахунок балансування навантаження, планування пріоритетів або використання довірчих значень, оскільки дуже складно точно визначити за такий короткий час, що дані, відправлені вузлом, є підробленими або законними. Отже, підходи з другої категорії надійніші, оскільки при використанні цих підходів немає шансів на втрату достовірних даних. Пропонована система відноситься до другої категорії.

Необхідно встановити правила потоку з дедалі більшою кількістю співпадаючих полів для детального управління і моніторингу статистики даних. Для цієї мети специфікація OF визначає набір за замовчуванням з 45

співпадаючих полів [2]. Більш того, у міру збільшення кількості співпадаючих полів для потоків до контролера буде надходити більше трафіку в формі повідомлень про пакетний вхід, і контролер буде використовувати більше ресурсів для їх обробки. Під час звичайного трафіку SDN відмінно працює з великою кількістю співпадаючих полів; проте, коли відбувається DoS-атака, кількість пакетів, відправлених по каналу управління, буде експоненціально збільшуватися. Ця атака вплине на SDN наступним чином:

1) Час відповіді від пункту призначення збільшиться
2) Завантаження ЦП контролера збільшиться
3) Трафік каналу управління збільшиться.

Щоб запустити DoS-атаку, зловмисник генерує підроблені запити маршруту, відправляючи підроблені пакети даних в різні місця призначення. Після прийому цих пакетів даних перемикачі OF, які знаходяться в межах шляху, відправляють повідомлення Packet-In контролера SDN. У відповідь контролер відправляє повідомлення Flow-Add комутаторів для пересилання даних до місця призначення. Кількість керуючих повідомлень (Packet-In і Flow-Add), створених в результаті кожного помилкового запиту, може бути розрахована за допомогою рівняння (3.1). Збільшення кількості підроблених запитів призведе до генерації більшої кількості пакетів управління, через що ресурси контролера будуть насичені, а його здатність обробляти запити знизиться. Тепер, щоб зменшити вплив DoS-атаки, важливо зменшити кількість керуючих повідомлень, оскільки кількість керуючих повідомлень прямо пропорційно завантаженню ЦП контролера.

Щоб зменшити кількість керуючих повідомлень під час DoS-атаки, пропонується модель установки паралельного потоку (PFI), змінюючи поведінку контролера з лінійного на паралельне для установки правила потоку. Традиційний контролер SDN відповідає тільки комутатору, від якого він отримує повідомлення Packet-In, як описано в алгоритмі 1; тоді у пропонованій моделі контролер відправляє повідомлення Flow-Add всім комутаторам, які знаходяться на шляху між джерелом і місцем призначення.

Це тому, що він знає, що ці включені перемикачі вимагатимуть розкрити шлях до місця призначення в майбутньому. Щоб перетворити поведінку контролера з лінійного в паралельну, функція обробки повідомлення Packet-In змінена таким чином, що вона становить список перемикачів, які лежать на шляху від джерела до місця призначення,

Пропонована модель пояснюється на рис. 3.2 з прикладом, який показує тимчасові інтервали для передачі даних від джерела (Host-1) до місця призначення (Host-8). У момент t1 хост-1 відправляє дані комутатора-D, який шукає в своїй таблиці потоків можливу наявність відповідного правила потоку для пересилання даних до місця призначення. Якщо не вдається знайти правило потоку, Switch-D відправляє повідомлення Packet-In контролера в момент t2. Контролер обчислює повний шлях від джерела до місця призначення і відправляє правила потоку всім комутаторам (D, B, A, C і G), присутнім на шляху в момент часу t3. У момент t4 данні переміщаються з Switch-D на Switch-G через комутатори B, A і C і, нарешті, на Host-8, оскільки правила потоку для пересилання даних вже встановлені на них. У пропонованому підході важливо відзначити, що контролер відправляє правила потоку тільки тим комутаторам, які включені в шлях між початковим і цільовим хостами. Таким чином, контролер не буде пересилати правила потоку комутаторів Switch-E і Switch-F, тому що вони не включені в шлях.

ONOS, RYU and POX.

```
1:  Src → newPkt;
2:  Send(Pkt) → InPort;
3:  for all Switches ∈ Path from Src to Dst do
4:     InPort ← Pkt;
5:     if Pkt.Header ∈ Flow_Table then
6:        Update.Counters();
7:        Send(Pkt) → OutPort;
8:     else
9:        Packet_In(Pkt.Header);
10:       Send(Packet_In) → Controller;
          // Lines (11-14) will be executed on controller
11:       identify next_hop;
12:       new Flow_Add;
13:       Flow_Add.OutPort ← next_hop;
14:       Send(Flow_Add) → Switch;
15:       Flow_Table ← Flow_Add;
16:       Update.Counters();
17:       Send(Pkt) → OutPort;
18:    end if
19: end for
20: OutPort → Dst;
```

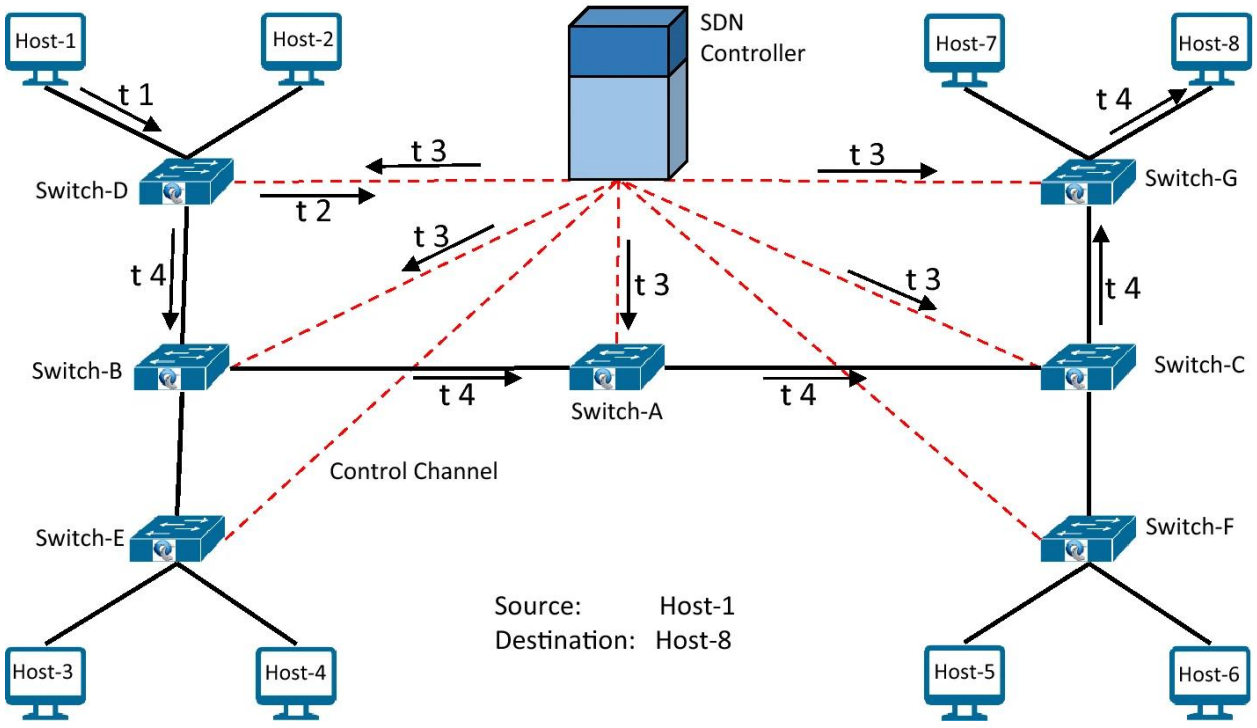


Рис. 3.2 Робота пропонованої системи паралельної установки

Згідно запропонованої моделі, як описано в алгоритм, одного повідомлення Packet-In досить для установки правил потоку на всіх комутаторах, включених в шлях від джерела до пункту призначення, тому кількість повідомлень OF по каналу управління для шляху може бути розрахована з модифікованої форми рівняння.

Розглянемо інший сценарій, в якому є 8 перемикачів на шляху від джерела до місця призначення. Як і в SDN, кожен комутатор на шляху відправляє повідомлення Packet-In контролера, щоб правило потоку перенаправляло дані від джерела до місця призначення. У відповідь на кожне повідомлення Packet-In контролер відправить повідомлення Flow-Add, що містить інструкції з пересилання даних до місця призначення. Отже, всього буде 16 повідомлень OF (8 повідомлень Packet-In і 8 Flow-Add), і якщо час обробки кожного пакета вважається рівним 1 мс, то час встановлення шляху буде 16 мс. Беручи до уваги, що в пропонованій моделі PFI тільки одне повідомлення Packet-In буде відправлено до контролера від першого комутатора на шляху, у відповідь на яке контролер відправить повідомлення Flow-Add всім 8 комутаторам, які лежать на шляху від джерела в пункт призначення. Отже, буде 9 повідомлень OF (1 повідомлення Packet-In і 8 повідомлень Flow-Add), а час встановлення шляху складе 9 мс.

3.3 Верифікація результатів дослідження

У таблиці 3.1 показані повідомлення OF для різної кількості комутаторів на шляху від джерела до місця призначення.

Таблиця 3.1

Повідомлення OF для різної кількості комутаторів на шляху від джерела до місця призначення

Кількість перемикачів	Установка з лінійним потоком			Пропонована установка з паралельним потоком		
	Пакетний вхід	Flow-Add	Всього	Пакетний вхід	Flow-Add	Всього
1	1	1	2	1	1	2
2	2	2	4	1	2	3
3	3	3	6	1	3	4
4	4	4	8	1	4	5
5	5	5	10	1	5	6
6	6	6	12	1	6	7
7	7	7	14	1	7	8
8	8	8	16	1	8	9

Пропонована модель PFI реалізована шляхом зміни механізмів маршрутизації модулів L2_learning [16] POX і Simple_switch_13 [15] RYU з лінійної на паралельну для OpenFlow [2] версій 1.1 та 1.3 відповідно. Для оцінки запропонованої моделі все експерименти виконуються шляхом емуляції топології мережі, як показано на рис. 3.2, і з використанням Mininet (версія 2.3.0) віртуальна мережа, встановлена на віртуальній машині і з'єднує її з віддаленими контролерами POX і RYU, що працюють на іншій віртуальній машині. Для генерації звичайного трафіку на Host-2 і Host-4 запускається сценарій, який відправляє TCP-трафік на Host-7 і Host-5 відповідно, який змінює порт призначення кожні 5 секунд, щоб запросити нове правило потоку від контролера.

Атака DoS запускається шляхом виконання сценарію на вузлі 3, який вибирає вузол з випадково згенерованого списку IP-адрес в межах мережевого діапазону і відправляє пакет даних на його випадковий порт через інтервал 0,01 с, так що кожен пакет вимагає нове правило від контролера. Продуктивність запропонованої моделі PFI порівнюється з алгоритмами

маршрутизації за замовчуванням POX і RYU. На різних тестах, таких як час відгуку, завантаження ЦП контролера, пропускна здатність каналу управління і запити потоку, відправлені на контролер. Результати кожного тесту обговорюються нижче для обох контролерів (POX і RYU) з атакою DoS і без неї.

Час відгуку

Це проміжок часу між відправленням пакета і отриманням відповіді від пункту призначення. Час відгуку розраховується шляхом відправки повідомлення ping від «Хост-1» всім іншим хостам. Експеримент повторювали кілька разів, щоб обчислити середній час відгуку.

Рис. 3.3 розкриває середній час відгуку для кожного хоста для контролерів POX і PFI без DoS-атаки (пунктирна смуга і хвильова смуга відповідно) і з DoS-атакою (діагональна смуга і перекреслена лінія відповідно). Більш короткі смуги для PFI і PFI-DoS можна спостерігати в порівнянні з смугами для POX і POX-DoS відповідно, що показує, що модель PFI має більш короткий час відгуку в порівнянні з POX майже для всіх хостів. Середній час відгуку POX і PFI без DoS-атаки становить 38,26 мс і 26,29 мс відповідно для всіх хостів, в той час як середній час відгуку POX і PFI з DoS-атакою становить 52,14 мс і 39,96 мс відповідно. Таким чином, пропонована система має на 31,29% менше часу відгуку при відсутності DoS-атаки і на 23,36% менше часу відгуку при наявності DoS-атаки.

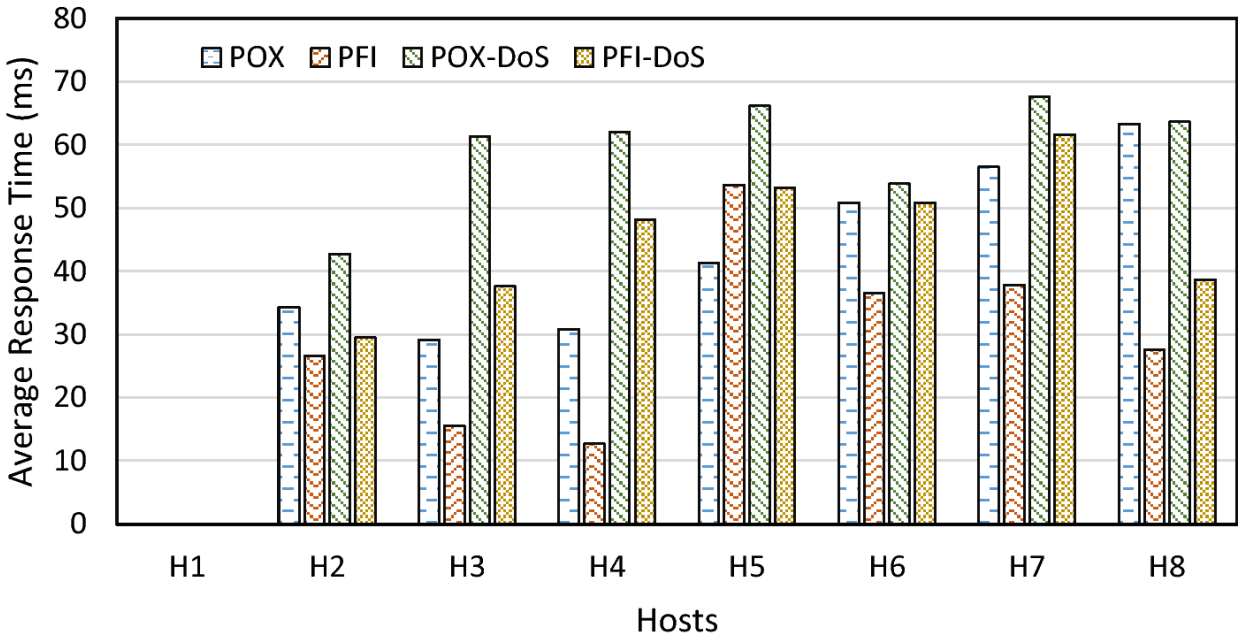


Рис. 3.3 Середній час відгуку для кожного хоста для контролерів POX і PFI без DoS-атаки (пунктирна смуга і хвильова смуга відповідно) і з DoS-атакою (діагональна смуга і перекреслена лінія відповідно)

Аналогічно, на на рис. 3.4 показано середній час відгуку для кожного хоста для контролерів RYU і PFI без DoS-атаки (пунктирна смуга і хвильова смуга відповідно) і з DoS-атакою (діагональна смуга і перекреслена лінія відповідно). Тут знову можна помітити, що стовпці для PFI і PFI-DoS коротше в порівнянні зі стовпцями для RYU і RYU-DoS відповідно, що ясно вказує на те, що модель PFI має більш короткий час відгуку в порівнянні з RYU. Тут середній час відповіді RYU і PFI без DoS-атаки становить 9,42 мс і 6,79 мс відповідно для всіх хостів, а середній час відгуку POX і PFI з DoS-атакою становить 15,09 мс і 12,31 мс відповідно. Таким чином, пропонована система має на 27,88% менше часу відгуку при відсутності DoS-атаки і на 18,43% менше часу відгуку при наявності DoS-атаки.

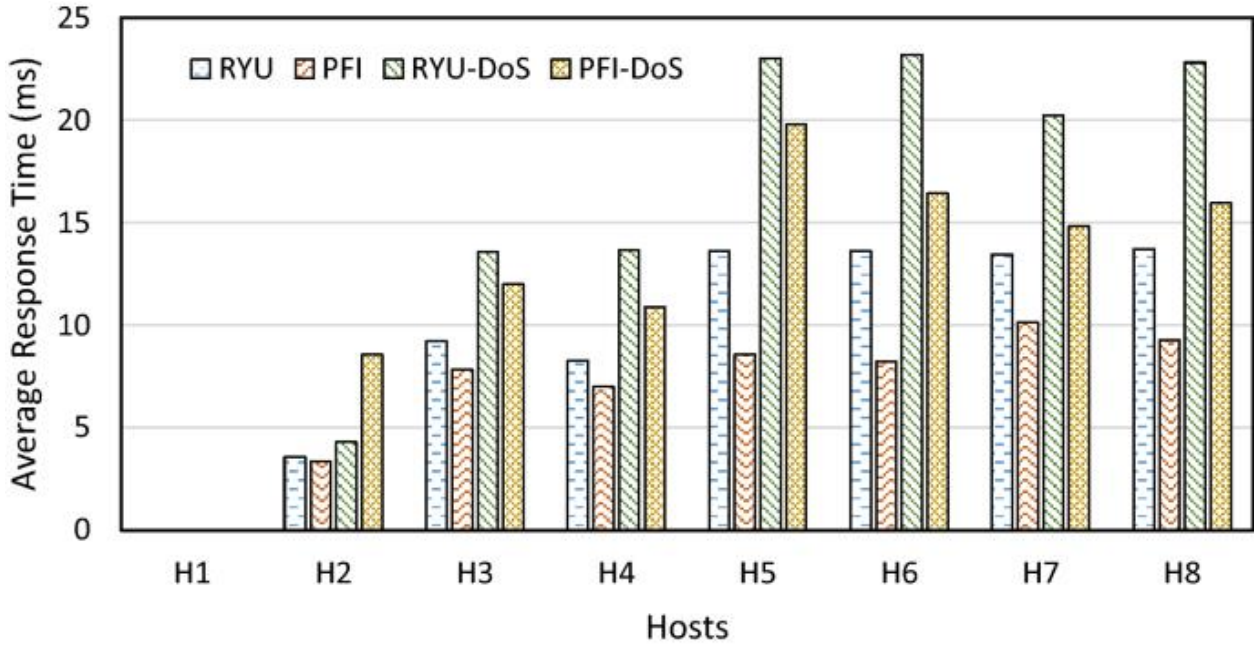


Рис. 3.4 Середній час відгуку для кожного хоста для контролерів RYU і PFI без DoS-атаки (пунктирна смуга і хвильова смуга відповідно) і з DoS-атакою (діагональна смуга і перекреслена лінія відповідно)

Завантаження процесора – це відсоток навантаження на контролери за період моделювання. Для розрахунку завантаження ЦП його по секундне використання реєструвалося протягом 300 с.

На рис. 3.5 чітко показано, що використання ЦП PFI-DoS (суцільна лінія зі сферами) нижче, ніж у POX-DoS (суцільна лінія з квадратами) під час DoS-атаки, тоді як під час звичайного трафіку завантаження ЦП обох PFI (пунктирна лінія) лінія зі сферами) і POX (пунктирна лінія з квадратами) майже рівні. Середнє завантаження ЦП для POX і PFI без DoS-атаки становить 5,87% і 6,11% відповідно. З іншого боку, середнє завантаження ЦП для POX і PFI при DoS-атаці становить 20,47% і 12,82% відповідно. Таким чином, запропонована модель має приблизно на 37,39% менше завантаження ЦП під час DoS-атаки.

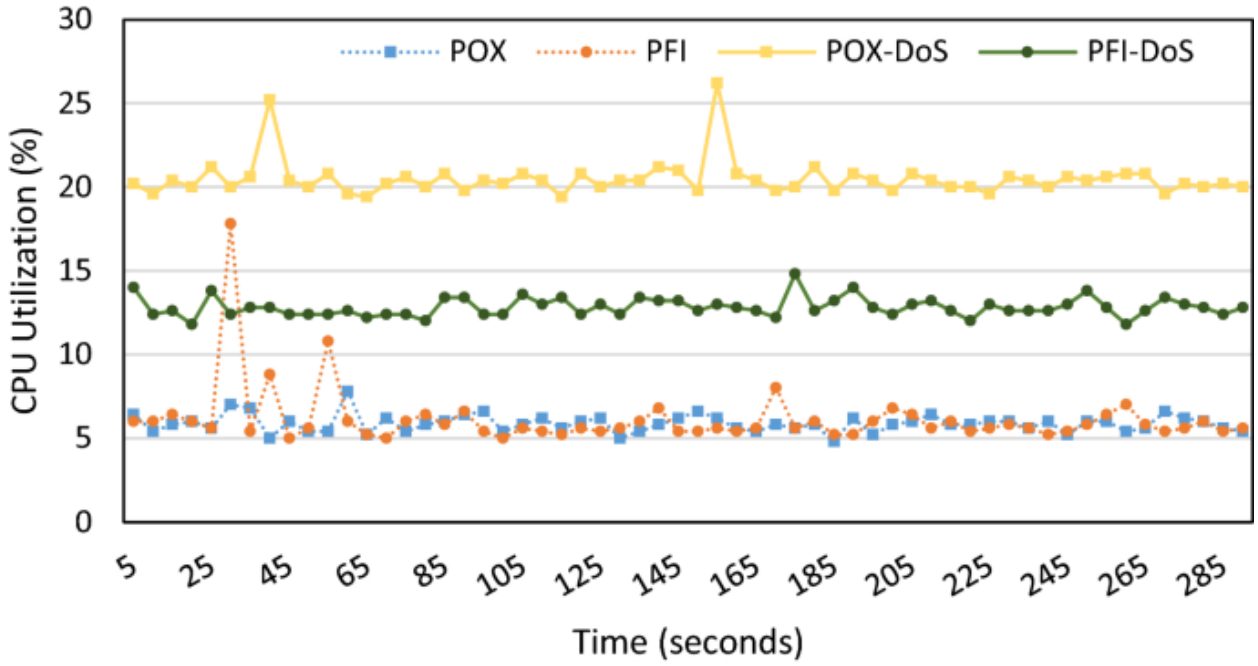


Рис. 3.5 Завантаження ЦП контролера POX

Аналогічним чином, на рис. 3.6, можна бачити, що середнє використання ЦП RYU (пунктирна лінія з квадратами) майже дорівнює кількості PFI (пунктирна лінія зі сферами) під час нормального руху, який є 7,04% і 6,96% відповідно. З іншого боку, під час DoS-атаки PFI-DoS (суцільна лінія зі сферами) має набагато нижче середнє завантаження ЦП у порівнянні з RYU-DoS (суцільна лінія з квадратами), яка становить 20,70% і 30% відповідно. Таким чином, запропонована модель має приблизно на 31,01% менше завантаження ЦП під час DoS-атаки. Причиною зниження завантаження ЦП є установка з паралельним потоком, при якій контролер повинен обробляти меншу кількість повідомлень Packet-In для всього шляху від джерела до пункту призначення. В результаті буде знижено завантаження ЦП.

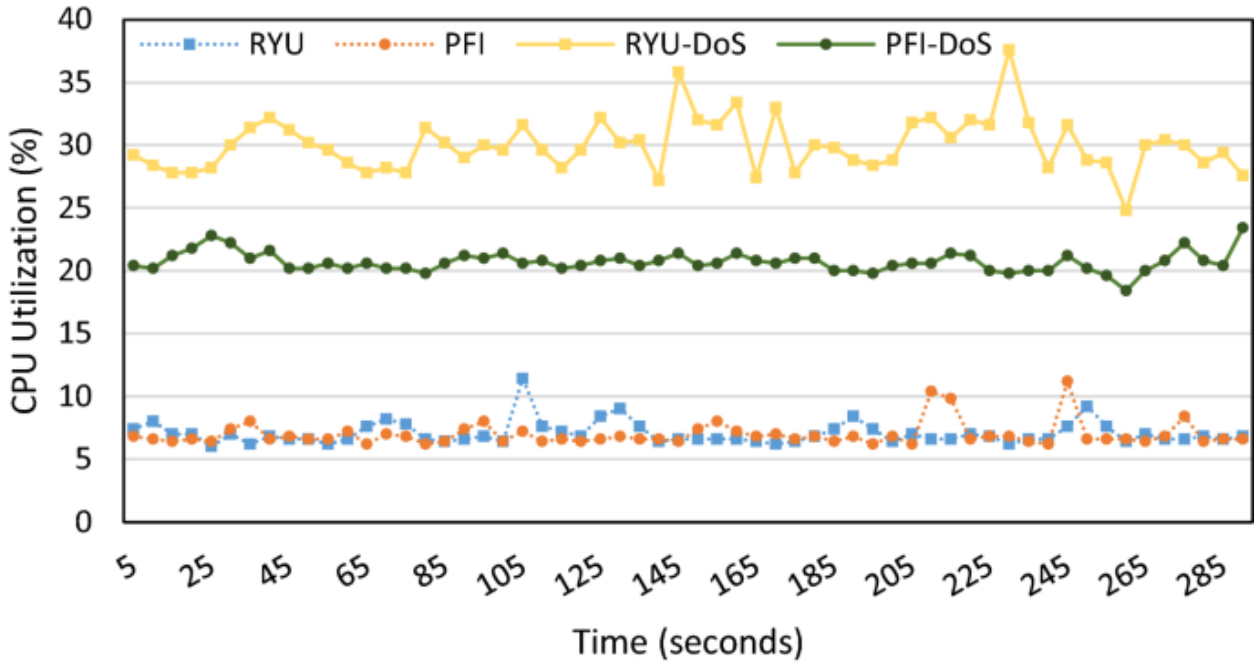


Рис. 3.6 Завантаження ЦП контролера POX

Смуга пропускання каналу управління – це обсяг даних, переданих по каналу управління між контролером і перемикачами. Щоб розрахувати обсяг даних, що відправляються з контролера, по секундна мережева статистика записувалася протягом 300 с.

На рис. 3.7 показаний середній обсяг даних, переданих між контролером і комутаторами для контролерів POX (пунктирна лінія з квадратами) і PFI (пунктирна лінія зі сферами) з нормальним трафіком 15,08 кбіт / с і 6,61 кбіт / с відповідно. З іншого боку, під час DoS-атаки середній обсяг даних, переданих для PFI-DoS (суцільна лінія зі сферами), становить 83,40 кбіт / с, що набагато менше, ніж у POX-DoS (суцільна лінія з квадратами) зі швидкістю передачі даних 269,43 кбіт / с. Таким чином, швидкість передачі даних для PFI і PFI-DoS знизилася приблизно на 56,17% і 69,04% відповідно.

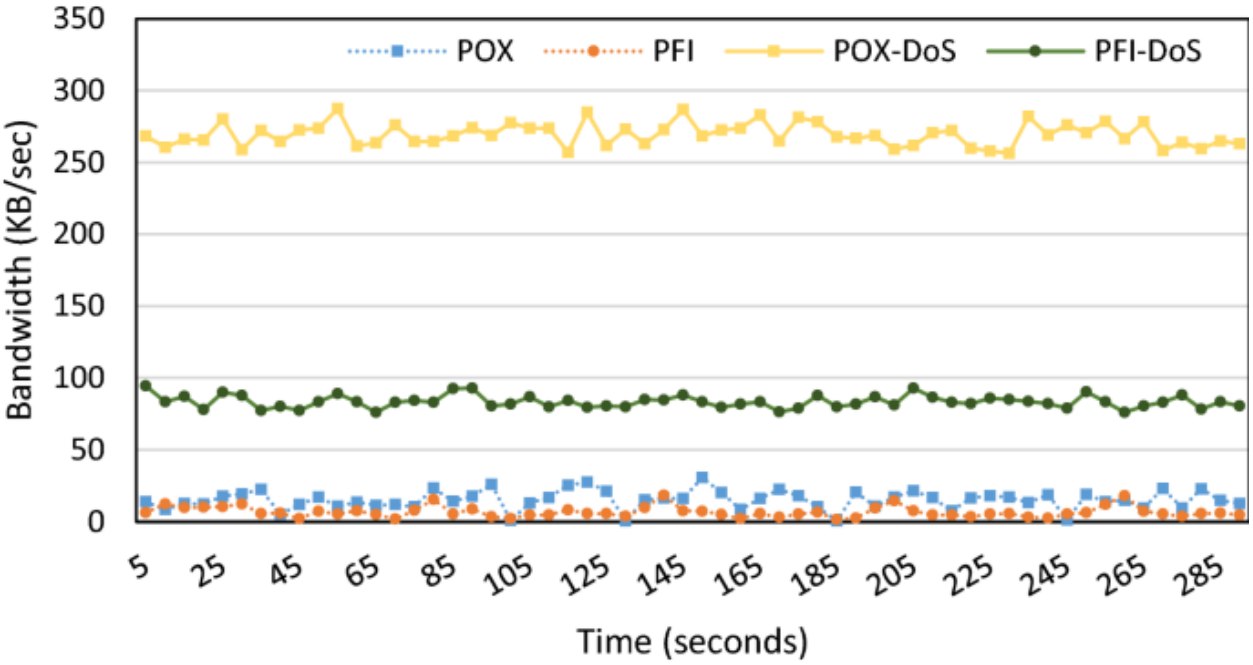


Рис. 3.7 Дані, надіслані по каналу управління для контролера POX

Таким же чином, на рис. 3.8 показує, що середня кількість даних, переданих між контролером і перемикачі для RYU (пунктирна лінія з квадратами) і PFI (пунктирна лінія зі сферами) контролерів з нормальним трафіком становить 7,0 кб / с і 4,31 кб / с відповідно. З іншого боку, під час DoS-атаки середній обсяг даних, переданих для PFI-DoS (суцільна лінія зі сферами), становить 134 кбіт / с, що набагато менше, ніж для RYU-DoS (суцільна лінія з квадратами) з даними швидкість 301 кбіт / с, що ще раз показує, що запропонована модель має на 38,46% і 55,62% менше швидкості передачі даних в порівнянні з RYU і RYU-DoS відповідно. Це скорочення використання смуги пропускання каналу управління відбувається через зменшення кількості повідомлень Packet-In, що відправляються на контролер з комутаторів.

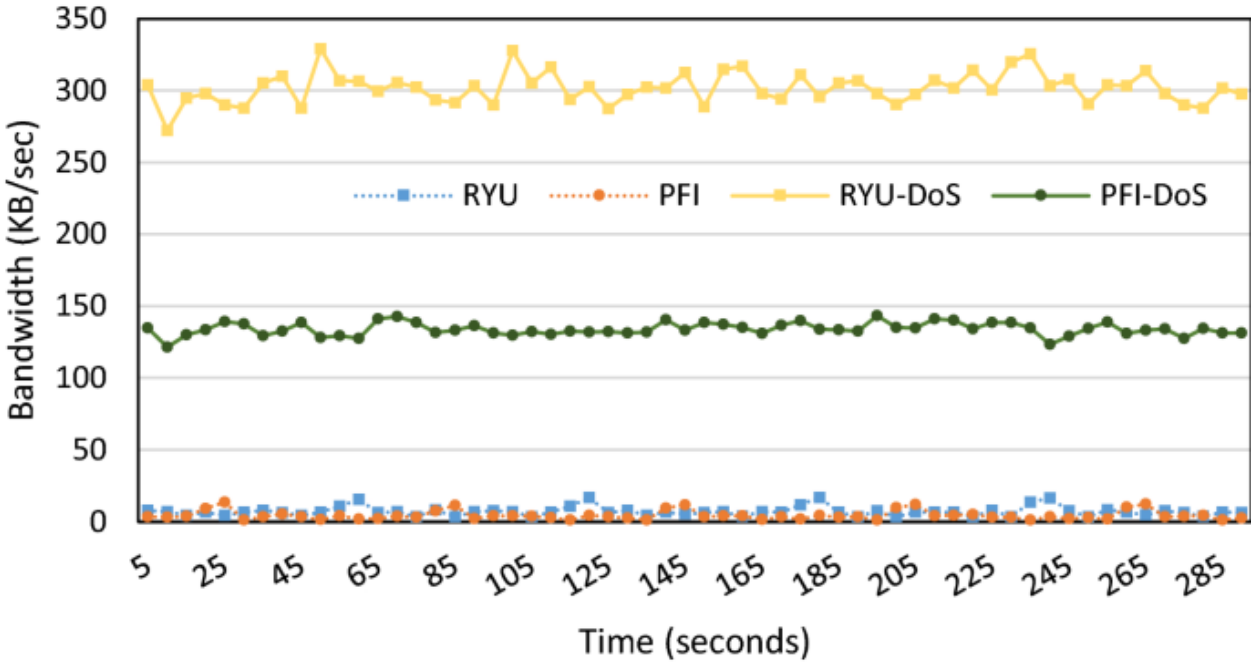


Рис. 3.8 Дані, надіслані по каналу управління для контролера RYU

Централізований характер SDN робить їх уразливими для DoS-атак, які можуть вивести з ладу всю мережу або її компонент, а також знизити її продуктивність. Вивчення існуючих методів протидії DoS-атак в SDN показує, що деякі з цих методів використовують складні методи, вимагають додаткового обладнання або модифікованих комутаторів. Крім того, ці методи можуть також викликати додаткову затримку в процесі маршрутизації і можуть додати більше трафіку в канал управління для цілей перевірки. Ці методи можуть відкидати допустимі пакети або не можуть виявити інтелектуальні DoS-атаки. Тому без цих компромісів дуже складно повністю нейтралізувати DoS-атаки. З огляду на всі перераховані вище проблеми, пропонується модель установки з паралельним потоком (PFI), щоб зробити SDN (особливо ті, які налаштовані для точного управління мережевим трафіком) більш стійкими до DoS-атак. Хоча пропонована модель не зупиняє DoS-атаку безпосередньо, вона ефективно зберігає смугу пропускання каналу управління і обчислювальну потужність контролера, щоб зробити її доступною для законних користувачів. Крім того, пропоновану модель можна використовувати з будь-яким існуючим методом, щоб зробити його більш

ефективним, а також збільшити пропускну здатність існуючої інфраструктури SDN. Результати наших експериментів показують, що пропонована модель PFI скорочує час на встановлення шляху, знижує обробку контролера і зменшує трафік каналу управління.

Висновки

Доведено ефективність управління безпекою інформаційних потоків мережі IoT за допомогою SDN.

За результатами розрахунку і наочному уявленню, можна сказати, що:

- при однакових числових значеннях, коефіцієнт готовності при використанні резервування вище ніж у нерезервованої системи;
- при використанні резервування $К_г$ менш залежний від інтенсивності виявлення відмов.

Резюмуючи все вище описане додам, що при організації мережі з використанням концепції SDN та резервування контролера, можна отримати надійну мережу, не враховуючи збільшення часу до виявлення відмови при роботі методів швидкого відновлення.

РОЗДІЛ 4
СТАРТАП ПРОЕКТУ

4.1 Опис ідеї проекту (товару, послуги, технології)

Таблиця 4.1

Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Метод управління безпекою інформаційних потоків мережі IoT за допомогою SDN	1. Виявлення атак	Підвищення рівня захисту мережі
	2. Розподіл трафіку	Захищеність інформаційної системи
	3. Підвищення рівня безпеки	Скорочення часу перевезення

Конкурентами є аналогічні методи та механізми управління безпекою інформаційних потоків мережі IoT за допомогою SDN. Основною відмінністю є те, що Метод управління безпекою інформаційних потоків мережі IoT за допомогою SDN реалізується таким чином, щоб забезпечити (по можливості) необхідну швидкість передачі повідомлень різних типів з урахуванням їх цінності та забезпечити безпеку даних.

Довгостроковими перспективами є:

- Збільшення кількості клієнтів, що будуть використовувати запропоновані методи управління безпекою інформаційних потоків мережі IoT за допомогою SDN.
- Додавання новітніх механізмів управління безпекою інформаційних потоків мережі IoT за допомогою SDN.

Потреби в стартовому фінансуванні:

Стартовий капітал = 25000 грн

Таблиця 4.2

Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№ п/п	Техніко-економічні характеристики ідеї	(потенційні) товари/концепції конкурентів				W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
		Мій проект	Конкурент1	Конкурент2	Конку-рент3			
1.	Бюджетне фінансування	розробка за рахунок розробника	розробка за рахунок бюджетних коштів	розробка комерційна	розробка за рахунок розробника	відсутність фінансування	часткова бюджетне фінансування	бюджетне фінансування
2.	Використання сучасної техніки	використовується сучасна техніка	використовується застаріла техніка	використовується техніка застарілої конфігурації	використовується сучасна техніка	сучасна комплектація технікою	часткова комплектація технікою	техніка застарілої конфігурації
3.	Належна матеріально-технічна база	розробко проводиться за власні кошти на приватному ПК	бюджетна установа	інформаційний центр	інформаційний центр	інформаційний центр	бюджетна установа	власні кошти на приватному ПК
4.	Підключення до Інтернету	є підключення до Інтернету	є підключення до Інтернету	є підключення до Інтернету	є підключення до Інтернету	без підключення до Інтернету	часткова підключення до Інтернету	є підключення до Інтернету
5.	Налагоджена система реклами продукту	продукт не рекламується	є реклама	продукт не рекламується	є реклама	не реклама	часткова реклама	рекламується
6.	Високий рівень розробки	запропоновані методи та алгоритми є досконалими	розробко не досконала та потребує доробок	запропоновані методи та алгоритми є досконалими	розробко не досконала та потребує доробок	розробко не досконала та потребує доробок	розробко є майже досконалою	запропоновані методи та алгоритми є досконалими

7.	Професіонали програмісти	розробка проводилася студентом	розробка проводилася групою професіоналів	розробка проводилася професіоналом програмістом	розробка проводилася професіоналом програмістом	розробка проводилася студентом	розробка проводилася професіоналом програмістом	розробка проводилася групою професіоналів
8.	Налагоджена співпраця із бізнес-структурами	ні	проводиться	ні	ні	ні	частково	проводиться

4.2 Технологічний аудит ідеї проекту

Визначення технологічної здійсненності ідеї проекту передбачає аналіз таких складових (табл. 4.3):

- за якою технологією буде виготовлено товар згідно ідеї проекту?
- чи існують такі технології, чи їх потрібно розробити/доробити?
- чи доступні такі технології авторам проекту?

Таблиця 4.3

Технологічна здійсненність ідеї проекту

№ п/п	Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
1	Метод управління безпекою інформаційних потоків мережі IoT за допомогою SDN	Технологія 1 (технологія надання послуги)	потрібно розробити	доступні
2		Технологія 2 (наявність бази досліджень)	наявні	доступні
3		Технологія 3 (база проведення досліджень (випробувань))	потрібно розробити	доступні
4		Технологія 4 (оформлення результатів дослідження)	потрібно розробити	доступні
Обрана технологія реалізації ідеї проекту: є можливою				

4.3 Аналіз ринкових можливостей запуску стартап проекту

Визначення ринкових можливостей, які можна використати під час ринкового впровадження проекту, та ринкових загроз, які можуть перешкодити реалізації проекту, дозволяє спланувати напрями розвитку проекту із урахуванням стану ринкового середовища, потреб потенційних клієнтів та пропозицій проектів-конкурентів.

Таблиця 4.4

Попередня характеристика потенційного ринку стартап-проекту

№ п/п	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од	2
2	Загальний обсяг продаж, грн/ум.од	34000
3	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу (вказати характер обмежень)	не має
5	Специфічні вимоги до стандартизації та сертифікації	ДСТУ В 7371:2013
6	Середня норма рентабельності в галузі (або по ринку), %	32

На основі проведеного дослідження є можливість стверджувати про привабливість проекту «Метод управління безпекою інформаційних потоків мережі IoT за допомогою SDN» для входження на ринок за попереднім оцінюванням.

Таблиця 4.2

Характеристика потенційних клієнтів стартап-проекту

№ п/п	Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
	Управління безпекою інформаційних потоків мережі IoT за допомогою SDN	Інформаційні служби, приватні підприємства	управління безпекою інформаційних потоків мережі IoT за допомогою SDN – програмісти/менеджери; зниження рівня загроз – системні програмісти;	відповідність ДСТУ ISO 9000:2015 Обов’язкова наявність сертифікатів

Таблиця 4.3

Фактори загроз

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
1	Агресивність конкурентів	вплив на систему	може порушити налагоджену систему розповсюдження
2	Нестабільність політичної ситуації в світі	балансування курсу	може порушити надійну систему постачальників
3	Висока вартість продукції	підвищення ціни	підвищить агресивність конкурентів
4	Економічні складності	відсутність фінансування	порушили фінансове забезпечення компанії

Таблиця 4.7

Фактори можливостей

№ п/п	Фактор	Зміст можливості	Можлива реакція компанії
1	Тривале існування	тривале існування на ринку	на ринку дає можливість виходу на нові ринки
2	Моніторинг потреб споживачів	розуміючи потреби споживачів, розширювати діапазон продукції, що випускається.	розширення діапазону продукції, що випускається.
3	Лібералізація торговельних бар'єрів	робота менеджменту	призведе до поліпшення налагодженої системи розповсюдження
4	Висока вартість продукції в порівнянні з ключовими конкурентами	встановлення високої ціни	утруднить вихід на нові ринки
5	Стабілізація бізнес-середовища	формування стабільного середовища	за рахунок стабілізації бізнес-середовища можна поліпшити фінансове забезпечення компанії

Таблиця 4.8

Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
1. Вказати тип конкуренції - монополія/олігополія/ монополістична/чиста	*Локальний/національний бізнес.* Глобальні сили є не досить вагомими по відношенню до локальних сил, які визначаються наявністю сертифікації, відповідності держ нормам і стандартам, регулюванням галузі перевезень державою.	працює в рамках управління безпекою інформаційних потоків мережі IoT за допомогою SDN
2. За рівнем конкурентної боротьби - локальний/національний/…	Локальний	Ведучи конкуренцію на локальному рівні, компанії необхідно прикласти належні зусилля для охоплення всього ринку Управління безпекою інформаційних потоків мережі IoT за допомогою SDN
3. За галузевою ознакою - міжгалузева/ внутрішньогалузева	*Внутрішньогалузева.* Конкуренція на ринку ведеться в інформаційній галузі України	Необхідно зосередити зусилля на пошуку конкурентних переваг, які дозволять компанії займати стійкі конкурентні позиції
4. Конкуренція за видами товарів: - товарно-родова - товарно-видова - між бажаннями	*Товарно-родова.* Конкуренція на рівні технології задоволення потреб. Існує конкуренція з іншими моделями, алгоритмами	методи управління безпекою інформаційних потоків мережі IoT за допомогою SDN
5. За характером конкурентних переваг - цінова / нецінова	*Нецінова.* При виборі алгоритмів та методів споживач звертає увагу на ефективність методів Управління безпекою інформаційних потоків мережі IoT за допомогою SDN. *Цінова*. Для значної частки споживачів ціна є визначальною при виборі.	Головною конкурентною перевагою є унікальність позиціонування методу управління безпекою інформаційних потоків мережі IoT за допомогою SDN
6. За інтенсивністю - марочна/не марочна	*Марочна.*	Диференціація методів та моделей за мотивом задоволення потреб споживачів

Таблиця 4.9

Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари-замінники
	Навести перелік прямих конкурентів	Визначити бар'єри входження в ринок	Визначити фактори сили постачальників	Визначити фактори сили споживачів	Фактори загроз з боку замінників
Висновки:	На ринку спостерігається тенденція до скорочення кількості підприємств і посилення конкуренції на ринку. Вступ України до СОТ відкрив дорогу іноземним виробникам. Великі компанії з іноземним капіталом постійно збільшують контрольованими частку ринку, поглинаючи конкурентів.	Бар'єри входу на ринок є порівняно незначними. Вартість організації бізнесу з виробництва сучасних механізмів Управління безпекою інформаційних потоків мережі IoT за допомогою SDN сягає 100 тис. дол. Обов'язковою є сертифікація продукції.	Існує чітка залежність від постачальників як якості продукції. Також ціна кінцевої продукції залежить від рівня сертифікаціїметоду Управління безпекою інформаційних потоків мережі IoT за допомогою SDN.	Споживачі мають широку географію і проживають переважно у містах. Покупка програмних додатків та алгоритмів реалізації Управління безпекою інформаційних потоків мережі IoT за допомогою SDN часто носить імпульсний характер.	Посилилася конкуренція зі сторони товарів субститутів – інших видів методів та алгоритмів Управління безпекою інформаційних потоків мережі IoT за допомогою SDN.

Отже, відповідно до наведеного вище аналізу головними силами, які діють на конкуренцію в галузі є постачальники та споживачі. Також в силу розвитку ринку все більшого значення набуває інтенсивність конкуренції між існуючими конкурентами та загроза зі сторони товарів-субститутуів.

Таким чином в межах структурного підходу до аналізу конкуренції тип конкуренції – *монополістична конкуренція*.

Таблиця 4.4

Обґрунтування факторів конкурентоспроможності

№	Фактор конкурентоспро-можності	Обґрунтування вибору
1	Частка ринку	Враховуючи той факт, що тип родового середовища в галузі – консолідований ринок, тобто існує група компаній, які контролюють разом понад 40% ринку, а також те, що інтенсивність суперництва між діючими конкурентами при низьких темпах зростання ринку є однією з головних сил, які діють на конкуренцію в галузі, одним з найважливіших факторів конкурентоспроможності виступає частка ринку, яку займає виробник. В таких умовах чим більше частка ринку, тим більшими ринковими можливостями володіє виробник.
2	Ціна	Чим вигіднішою є ціна для споживача, тим вірогідніше його вибір.
3	Асортимент	В умовах збільшення інтенсивності між існуючими конкурентами завоювання споживачів відбувається за рахунок нових методів та алгоритмів управління безпекою інформаційних потоків мережі IoT за допомогою SDN.
4	Доступ до каналів розподілу	Споживач далеко не завжди проявляє прихильність до певної категорії розробників і дуже схильний до експериментів. В цьому випадку завоювати лояльність споживача дуже складно і ще складніше її утримати. Тому для компаній-виробників ключовими чинниками успіху стає сильна дистрибуція, якісний торговий маркетинг і налагоджена система логістики.
5	Торговий маркетинг	
6	Рівень диференціації ТМ	В умовах ведення конкурентної боротьби на споживчому ринку, де попит є ірраціональним та існує велика кількість виробників і розробників при фактично відсутній різниці між товарами, що пропонуються, ключовим фактором успіху є здатність чітко диференціювати ТМ від ТМ конкурентів, надаючи споживачеві унікальну цінність.
7	Репутація виробника	Якщо компанія має бездоганну репутацію, особливо у сфері якості своєї продукції, то рівень довіри до неї зростає. Також репутація виробника важлива при виході на ринок з новими товарами, або при виході на нові сегменти, що полегшує позитивне сприйняття новинок.
8	Рівень лояльності до бренду	Чим вище рівень лояльності, тим більше компанія має прихильних, а значить постійних споживачів.
9	Унікальність позиціонування	В умовах монополістичної конкуренції, коли фактор диференціації ТМ є ключовим засобом ведення конкурентної боротьби, важливим є створення та підтримання унікального

№	Фактор конкурентоспро-можності	Обґрунтування вибору
		позиціонування, що створює певний захист від конкурентних зіткнень.
10	Маркетинговий бюджет	Від розміру маркетингового бюджету залежить здатність здійснювати маркетингову стратегію підприємства. Маркетингові заходи мають забезпечувати інші конкурентні переваги такі, як рівень диференціації, лояльності, репутація виробника, дистрибуція та просування в торгових точках.

Таблиця 4.5

Порівняльний аналіз сильних та слабких сторін «Метод управління безпекою інформаційних потоків мережі IoT за допомогою SDN»

№	Фактор конкурентоспроможності	Вагові значення фактора (1-20)	Рейтинг конкурентів у порівнянні з Метод управління безпекою інформаційних потоків мережі IoT за допомогою SDN						
			-3	-2	-1	0	1	2	3
1	Частка ринку	20							
2	Ціна	10							
3	Асортимент	18							
4	Доступ до каналів розподілу	15							
5	Торговий маркетинг	15							
6	Рівень диференціації ТМ	13							
7	Репутація виробника	12							
8	Рівень лояльності до бренду	14							
9	Унікальність позиціонування	15							
10	Маркетинговий бюджет	10							

Умовні позначки позицій конкурентів:

- *конкурент 1*
- *конкурент 2;*
- *конкурент 3.*

Отже, відповідно до проведеного аналізу можна сказати, що « Метод управління безпекою інформаційних потоків мережі IoT за допомогою SDN» має наступну позицію на ринку:

сильні сторони:

– індивідуальне позиціонування;

– підвищений рівень диференціації ТМ;

– добра репутація виробника;

слабкі сторони:

– максимальна ціна порівняно з конкурентами;

– торговий маркетинг.

Виділивши найвагоміші сильні та слабкі сторони « Метод управління безпекою інформаційних потоків мережі IoT за допомогою SDN» у порівнянні з основними конкурентами і з аналізу внутрішніх факторів та використовуючи результати аналізу маркетингових загроз та можливостей, складемо матрицю SWOT-аналізу (табл. 4.12.).

Таблиця 4.12

SWOT-аналіз стартап-проекту

Сильні сторони	**Слабкі сторони**
1. інфдивідуальне позиціонування; **2.** максимальний рівень диференціації **3.** позитивна репутація виробника; **4.** приналежність до української міжнародної компанії; **5.** відлагоджена система дистрибуції товару; **6.** наявність вертикальної інтеграції.	**1.** підвищена ціна порівняно з конкурентами. **2.** залежність маркетингової політики від українського власника; **3.** мінімальне самозабезпечення фінансовими ресурсами; **4.** відсутність чітко вираженої маркетингової стратегії, непослідовність в її реалізації.
Можливості	**Загрози**

1. Можливість зміцнення іміджу **2.** Можливість підвищення обсягів реалізації **3.** Можливість підвищення обсягів продаж за рахунок експансії в регіони	**1.** Загроза працювати без прибутку скорочення платоспроможного попиту **2.** Загроза втрати споживачів внаслідок підвищення тиску зі сторони товарів-субститутів **3.** Загроза збільшення цін

З результатів SWOT-аналізу видно, що найбільш негативний вплив на діяльність « Метод управління безпекою інформаційних потоків мережі IoT за допомогою SDN» на ринку чинить ринкове середовище. Це, перш за все, пов’язано із наслідками фінансово-економічної кризи в країні.

В свою чергу, така ситуація супроводжувалася зменшенням темпів приросту галузі, виходом з ринку менш сильних дрібних та регіональних виробників, приходом на ринок транснаціональних компаній, що збільшило інтенсивність конкуренції між діючими учасниками ринку України.

Було визначено, що найбільшою загрозою для «Метод управління безпекою інформаційних потоків мережі IoT за допомогою SDN» є загроза падіння прибутковості внаслідок скорочення попиту.

Таблиця 4.6

Альтернативи ринкового впровадження стартап-проекту

№ п/п	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	Ймовірність отримання ресурсів	Строки реалізації
1.	Використання засобів стимулювання збуту та мерчандайзингу в торгових точках для збільшення продаж	Дозволяє суттєво збільшити обсяги продаж	до місяця
2.	Розширення асортиментної лінійки	Можливість залучення нових	до пів року

		споживачів за рахунок новинки	
3.	Збільшення представленості	Можливість розширення охоплення цільової аудиторії	до року

Найоптимальнішою є перша альтернатива

4.4 Розроблення ринкової стратегії проекту

Розроблення ринкової стратегії першим кроком передбачає визначення стратегії охоплення ринку: опис цільових груп потенційних споживачів (табл.4.14).

Таблиця 4.7

Вибір цільових груп потенційних споживачів

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1	Метод управління безпекою інформаційних потоків мережі IoT за допомогою SDN	готовий	високий	мінімальна	простий
2	Зменшення часу на перевезення	готовий	високий	максимальна	простий
3	Підвищення якості побудови маршрутів	готовий	високий	середня	простий
Які цільові групи обрано: стратегію диференційованого маркетингу					

Таблиця 4.8

Визначення базової стратегії розвитку

№ п/п	Обрана альтернатива розвитку проекту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку*
1	**Стратегія диференціації**	передбачає надання товару важливих з точки зору споживача відмітних властивостей, які роблять товар відмінним від товарів конкурентів. Така відмінність може базуватися на об’єктивних або суб’єктивних, відчутних і невідчутних властивостях товару(у ширшому розумінні – комплексі маркетингу), бути реальною або уявною.	Реалізація цієї стратегії вимагає, як правило, більш високих витрат. Проте успішна диференціація дозволяє компанії домогтись більшої рентабельності за рахунок того, що ринок готовий прийняти більш високу ціну (цінову премію бренду).	Інструментом реалізації стратегії диференціації є ринкове позиціонування.

Таблиця 4.9

Визначення базової стратегії конкурентної поведінки

№ п/п	Чи є проект «першопрохідцем» на ринку?	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, і які?	Стратегія конкурентної поведінки*
	Ні	залучати нових так і забирати існуючих у конкурентів	частково	наслідування лідеру

Таблиця 4.10

Визначення стратегії позиціонування

№ п/п	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспроможні позиції власного стартап-проекту	Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових)
1	Відповідність чинним нормативам	Наслідування лідеру	Реалізація цієї стратегії вимагає, як правило, більш високих витрат. Проте успішна диференціація дозволяє компанії домогтись більшої рентабельності за рахунок того, що ринок готовий прийняти більш високу ціну (цінову премію бренду).	Унікальність Доступна ціна Реалізація нових методів

Висновки

Відповідно до проведеного аналізу можна сказати, що « Метод управління безпекою інформаційних потоків мережі IoT за допомогою SDN» має наступну позицію на ринку:

сильні сторони:

– індивідуальне позиціонування;
– підвищений рівень диференціації ТМ;
– добра репутація виробника;

слабкі сторони:

– максимальна ціна порівняно з конкурентами;
– торговий маркетинг.

Виділивши найвагоміші сильні та слабкі сторони « Метод управління безпекою інформаційних потоків мережі IoT за допомогою SDN» у порівнянні з основними конкурентами і з аналізу внутрішніх факторів та використовуючи результати аналізу маркетингових загроз та можливостей, було складено матрицю SWOT-аналізу, Визначення базової стратегії конкурентної поведінки, Визначення стратегії позиціонування, Вибір цільових груп потенційних споживачів

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

У межах даної роботи досліджено метод управління безпекою інформаційних потоків мережі IoT за допомогою SDN.

В ході дослідження були вивчені і описані основні положення концепції SDN, що пропонують рішення проблем існуючої архітектури мережі Інтернет, які дозволять модернізувати мережу, знизити витрати на розвиток і експлуатацію, прискорити впровадження нових мережевих послуг.

Незважаючи на те, що реалізація SDN ще не до кінця опрацьована, згідно з результатами досліджень світового телекомунікаційного ринку найближчим часом SDN займе провідне місце як на світовому, так і на вітчизняному ринку. Тому як ніколи важливо враховувати вразливості даної технології в аспекті надійності, такі як централізоване управління мережею, де контролер SDN є єдиною точкою відмови.

На основі проведених досліджень, представлених в даній роботі, можна сказати що подолати цей недолік допоможуть різні механізми забезпечення надійності мережі. У зв'язку з цим, автором представлені основні методи забезпечення відмовостійкості, такі як резервування і перемаршрутизація. Обидва ці методи дозволяють забезпечити необхідний користувачем показник готовності з'єднання або показник готовності різних послуг, що надаються.

У роботі розглянуті основні процедури резервування, які можуть використовуватися в мережах зв'язку, а також проаналізовано механізм перемаршрутизації. Представлена узагальнена характеристика методів захисту від відмов.

Крім використання заявлених алгоритмів, автором пропонується ряд робіт пов'язаних із дослідженням підвищення надійності в мережах SDN при якому необхідно враховувати правильне розміщення контролерів при широкомасштабному розгортанні мережі.

При оцінці впливу резервування на надійність мережі SDN, представленої в роботі, використовувалися аналітичні методи моделювання засновані на теорії випадкових процесів. Дані методи були застосовані для

досліджуваної мережі при відсутності резервування і при резервуванні контролера, зроблені відповідні висновки про вплив резервування на коефіцієнт готовності.

Для дослідження надійності мережі при використанні методу відновлення було проведено аналіз оригінального способу відновлення протоколу OpenFlow. Представлені алгоритми перемаршрутизації, які можна використовувати для обчислення маршруту в разі виникнення відмови. В додаток дослідником пропонується використовувати спосіб відновлення по протоколу OpenFlow із застосуванням розширення згідно OpenQoS. OpenQoS використовує пересилання на основі потоку, на відміну від сучасних мереж. Таким чином перестроювання маршруту при відмові відбувається не тільки по незачепленим відмовою маршрутом, а й відповідно до вимог OpenQoS.

Системи на основі SDN є перспективними і заслуговують уваги, так як дозволяють зробити якісно-новий крок на шляху до необхідної по функціональності мережі.

Всі завдання, поставлені в даній дипломній роботі, досягнуті. В роботі представлений не тільки детальний аналіз і зроблені розрахунки для досліджуваної мережі, але також розглянуті перспективні напрямки дослідження пов'язані з підвищенням якості функціонування мереж.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. SDN basics: Understanding centralized control and programmability [Електронний ресурс] / / TechTarget. – Режим доступу: https://searchsdn.techtarget.com/tip/SDN-basics-Understanding-centralizedcontrol-and-programmability, вільний. - Загл. з екрану. (20.11.2020).
2. Nadeau T. SDN – Software Defined Networks. / T. Nadeau – CA.: published by O'reilly media, 2013. – 80 с. 3. Goransson P. Software Defined Networks: A Comprehensive Approach. / P. Goransson. – MA.: Elsevier Inc, 2014. – С. 215.
3. Azodolmolky S. Software Defined Networking with OpenFlow / S. Azodolmolky – UK.: Packt Publishing, 2013. – 148 с.
4. Software-Defined Networking (SDN) Definition [Електронний ресурс] / / ONF. – Режим доступу: https://www.opennetworking.org/sdn-definition/, вільний. – Загл. з екрану. (28.11.2020).
5. Критерії оцінки мереж [Електронний ресурс] / / om.net.ua. – Режим доступу: http://om.net.ua/9/9_6/9_68601_kriterii-otsenki-setey.html, вільний. - Загл. з екрану. (03.12.2020).
6. Monge A. MPLS in the SDN Era. / Monge A. – CA.: published by Juniper networkds, 2013. – 194 с.
7. Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud / Stallings W. – CA.: published by Pearson, 2015. – 116 с.
8. Doherty J. SDN and NFV Simplified / Doherty J. – CA.: published by Addison-Wesley Professional, 2016. – 173 с.
9. Tiwari V. SDN and OpenFlow for Beginners with Hands on Labs / Tiwari V. – CA.: published by Amazon Digital Services LLC, 2013. – 15 с
10. Zolanvari M. SDN for 5G / Maede Zolanvari // Rotation October 2015. https://www.cse.wustl.edu/~jain/cse570-15/ftp/sdnfor5g.pdf
11. Лунтовський А.О. Застосування технологій SDN для програмної реалізації провайдерського ядра систем мобільного зв'язку 5G майбутнього покоління / А. О. Лунтовський, А. І. Семенко // Зв'язок, 2014. № 3. С. 13-19.

12. Sarigiannidis P. Hybrid 5G optical-wireless SDN-based networks, challenges and open issues / Panagiotis Sarigiannidis, Thomas Lagkas, Stamatia Bibi // IET Networks – Volume: 6, Issue: 6, p. 141-148 – DOI: 10.1049/iet-net.2017.0069. 2017.

13. Mohammed A. Alqarni Benefits of SDN for Big data applications / Mohammed A. Alqarni // 14th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT (HONET-ICT), IEEE – Electronic ISSN: 1949-4106 – DOI: 10.1109/HONET.2017.8102206. 2017.

14. Bera S. Software-Defined Networking for Internet of Things: A Survey / Samaresh Bera, Sudip Misra, Athanasios V. Vasilakos // IEEE Internet of Things Journal, Volume: 4, Issue: 6, Dec. 2017

15. Sun S. Integrating Network Function Virtualization with SDR and SDN for 4G/5G Networks / Songlin Sun, Michel Kadoch, Liang Gong, Bo Rong // IEEE Network 29(3): p.54-59 - DOI10.1109/MNET.2015.7113226. 2015. 28 РИ, 2018, №1

16. Hakiri A. Leveraging SDN for The 5G Networks: Trends, Prospects and Challenges / Akram Hakiri, Pascal Berthou // arXiv:1506.02876. 2015.

17. Mendiola A. A Survey on the Contributions of SoftwareDefined Networking to Traffic Engineering / Alaitz Mendiola, Jasone Astorga, Eduardo Jacob // DOI: 10.1109/COMST.2016.2633579 - IEEE Communications Surveys & Tutorials -Volume: 19, Issue: 2. P. 918-953. 2017.

18. About ONF Mission / Official website of the Open Networking Foundation. https://www.opennetworking.org/mission/

19. Shengru Li. Protocol Oblivious Forwarding (POF): Software-Defined Networking with Enhanced Programmability / Shengru Li, Daoyun Hu, Wenjian Fang // DOI: 10.1109/MNET.2017.1600030NM – IEEE Network – Volume: 31, Issue: 2, March/April 2017. P. 58-66

20. Скулиш М. А. Метод контролю якості обробки інформаційних потоків у мережі 5G / М. А. Скулиш, А. А. Заставенко // Вісник Національного

університету "Львівська політехніка". Радіоелектроніка та телекомунікації, 2016, № 849, с. 265-273.

21. Mancuso V. A prototyping methodology for SDN-controlled LTE using SDR / Vincenzo Mancuso, Christian Vitale, Rohit Gupta, Karamvir Rathi, Arianna Morelli – January 2017 – https://www.researchgate.net/publication/312661126_A_prototyping_methodology_for_SDN-controlled_LTE_using_SDR

22. Mateo P. A Context-aware Model for the Analysis of User Interaction and QoE in Mobile Environments / P. Mateo, D. S. Ruiz, G. M. Perez // International Journal of Human-Computer Interaction. – 2014. – Vol. 30I. 12. – Norwood, N.J, USA : Ablex Pub. – P. 946-964.

23. Теленик С. Ф. Зведення метрик оцінювання рівня обслуговування користувачів на основі експертних оцінок [Текст] / С. Ф. Теленик, О. І. Ролік, О. М. Моргаль, О. С. Квітко // Вісник Вінницького політехнічного інституту. – 2011. – № 1. – С. 112–123.

24. Nanduri R. Job Aware Scheduling Algorithm for MapReduce Framework / R. Nanduri, N. Maheshwari, R. Raja, V. Varma // 3rd IEEE International Conference on Cloud Computing Technology and Science.– Athens, Greece : IEEE Press, 2011. – P. 724–729.

25. Карпенко А. П. Современные алгоритмы поисковой оптимизации. Алгоритмы, вдохновленные природой / А. П. Карпенко. – Москва : МГТУ им. Н. Э. Баумана, 2014. – 446 с

26. SLA Management Handbook / TM Forum Publication. – Morristown, NJ, USA : TeleManagement Forum, 2001. – 141 p.

27. Varela M. From Service Level Agreements (SLA) to Experience Level Agreements (ELA): The challenges of selling QoE to the user [Text] / M. Varela, P. Zwickl, M. Xie, H. Schulzrinne [et al.] // Communication Workshop (ICCW), 2015 IEEE International Conference on 8–12 June 2015. – London, UK : IEEE Press, 2015. – P. 1741–1746.

28. Москаленко В.В. Інтелектуальна система керування розподілом ресурсів телекомунікаційної мережі /В.В. Москаленко, С.В. Пимоненко // Матеріали III міжнародної науково-практичної конференції «Обчислювальний інтелект». – Черкаси : ЧДТУ. – 2015. – С. 249. 310

29. N. Shah, "Understanding network processors," Tech. Rep. Version 1.0, EECS, University of California, Berkeley, September 2001.

30. Ладиженський Ю.В. Грищенко В.И. Моделирование сетевых процессоров пакетной обработки данных. Матеріали міжнародної науковопрактичної конференції „Інтернет – Освіта – Наука - 2006”, м. Вінниця, 10 – 14 жовтня 2006 р., т. 2, стр. 417-422.

31. Samarjit Chakraborty, Simon Kunzli, Lothar Thiele et. al. Performance evaluation of network processor architectures: combining simulation with analytical estimation. Computer Networks: The International Journal of Computer and Telecommunications Networking. Vol. 41, Iss. 5 (Apr. 2003). 2003. pp. 641 – 665.

32. M. Gries, C. Kulkarni, C. Sauer, K. Keutzer. Comparing Analytical Modeling with Simulation for Network Processors: A Case Study. Design Automation and Test in Europe (DATE), Munich, Germany, March 2003.

33. Tilman Wolf, Mark A. Franklin, "Performance Models for Network Processor Design," IEEE Transactions on Parallel and Distributed Systems, vol. 17, no. 6, pp. 548-561, Jun., 2006.

34. M. Ahmadi, S. Wong, A Performance Model for Network Processor Architectures in Packet Processing Systems, Proceedings of the 19th International Conference on Parallel and Distributed Computing and Systems (PDCS 2007), pp. 176-181, Cambridge, Massachusetts, USA, November 2007

35. F. Baker et al. RFC1812 – Requirements for IP Version 4 Routers. Cisco Systems. June 1995.

36. В. Г. Олифер, Н. А. Олифер. Компьютерные сети. Принципы, технологии, протоколы.3-е изд.-2006, СПб, Изд. дом "Питер", 958 стр.

37. P. Ferguson and G. Houston, Quality of Service: Delivering QoS on the Internet and in Corporate Networks, John Wiley & Sons, 1998.

38. Canfora, G., Di Penta, M., Esposito, R., Villani, M.L.: An Approach for QoS-aware Service Composition based on Genetic Algorithms. In: GECCO 2005, ACM Press, New York (2005) 311

39. Canfora, G., Di Penta, M., Esposito, R., Perfetto, F., Villani, M.L.: Service Composition (re)Binding Driven by Application-Specific QoS. In: Dan, A., Lamersdorf, W. (eds.) ICSOC 2006. LNCS, vol. 4294, Springer, Heidelberg (2006)

40. Nguyen, X.T., Kowalczyk, R., Han, J.: Using Dynamic asynchronous aggregate search for quality guarantees of multiple Web services compositions. In: Dan, A., Lamersdorf, W. (eds.) ICSOC 2006. LNCS, vol. 4294, Springer, Heidelberg (2006)

41. Trang, D. D. Fractal Analysis and Modeling of VoIP Traffic // D. D. Trang, B. Sonkoly, S. Molnar// Telecommunications Network Strategy and Planning Symposium. 2004. - Issue №1. - P. 123-130.

42. Crovella, M. E. Self-similarity in world wide web traffic: Evidence and possible causes / M. E. Crovella, A. Bestavros// IEEE/ACM Trans. Networking – 1997. Vol. 5, № 6. – P. 835-846.

43. Samorodnitsky, G. Stable Non Gaussian Random Processes: Stochastic Model swith Infinite Variance Электронный документ. / G. Samorodnitsky, M. Taqqu. Режим доступу: http://math.bu.edu/people/murad/stable-expanded.html - 08.12.2008

44. 11. R.I. ITU-T,910, "Subjective video quality assessment methods for multimedia applications, 1999

45. Book: Antoine Cornuéjols-Laurent Miclet. "Apprentissage artificiel: concepts et algorithms" EYROLLES, 2010.

46. D.K.Krishnappa, S.Khemmarat, M.Zink, "Planet Youtube: Global, measurement-based performance analysis of viewer;'s experience watching user generated videos," Local Computer Networks, Annual IEEE Conference on, pp. 948- 956, 2011 IEEE 36th Conference on Local Computer Networks, 2011.

47. 1G.Zhang, W. Jin, L. Hu, "Radar emitter signal recognition based on support vector machines," Control, Automation, Robotics and Vision Conference, (ICARCV), vol.2, no., pp. 826-831 Vol. 2, 6-9 Dec. 2004. 312

48. M.J. Islam, Q.M.J. Wu, M. Ahmadi, M.A. Sid-Ahmed, "Investigating the Performance of Naive- Bayes Classifiers and K- Nearest Neighbor Classifiers," Convergence Information Technology, International Conference, pp.1541-1546, 21-23 Nov. 2007.

49. M. Pal, P.M. Mather, "A comparison of decision tree and backpropagation neural network classifiers for land use classification," IEEE International Geoscience and Remote Sensing Symposium (IGARSS), vol.1, no., pp. 503-505 vol.1, 2002.

50. W.T. Aung, K..H.M Saw Hla, "Random forest classifier for multi-category classification of web pages," IEEE Asia-Pacific Services Computing Conference (APSCC), pp.372-376, 7-11 Dec. 2009.

51. J. C. S. Andrade, R. B. C. Ribeiro, R. S. Villaça, M. Martinello and C. A. S. Santos, "SANGN: A New Service Oriented Architecture for Provisioning of NGN Scalable Multimedia Services," 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), Krakow, 2018, pp. 504-511.

52. M. A. Barry, J. K. Tamgno, C. Lishou and M. B. Cissé, "QoS impact on multimedia traffic load (IPTV, RoIP, VoIP) in best effort mode," 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon-si Gangwon-do, Korea (South), 2018, pp. 694-700.

53. Филиппов А.К. Теоретические основы проектирования динамически реконфигурируемых систем обработки информации: учебн. пособ. / Филиппов А.К. – Владимир: Изд-во Владим. гос. ун-та, 2009. − 119 с.

54. Иванов А.И. О создании и применении проблемно-ориентированных комплексов, предназначенных для решения задач, обладающих высокой емкостной и временной сложностью / А.И. Иванов // Штучний інтелект. − 2004. − № 4. − С. 15 – 26.

55. Гузик В.Ф. Проблемно-ориентированные высокопроизводительные вычислительные системы: учебн. пособ. / В.Ф. Гузик, В.Е. Золотовский. − Таганрог: Изд-во ТРТУ, 1998. – 236 с. 313

56. Опанасенко В.Н. Высокопроизводительные реконфигурируемые компьютеры на базе FPGA / В.Н. Опанасенко // Проблеми інформатизації та управління: зб. наук. праць НАУ. – 2009. – Вип. 3 (27). – С. 114 – 118.

57. Палагин А.В. Проблемная ориентация в развитии компьютерных архитектур / А.В. Палагин, А.Ф. Кургаев // Кибернетика и системный анализ. − 2003. − № 4. − С. 167 − 180.

58. Палагин А.В. Об ЭВМ с виртуальной архитектурой / А.В. Палагин // Управляющие системы и машины. − 1999. − № 3. − С. 33 – 43.

59. Task Scheduling Onto Dynamic Large-Scale Parallel Cluster (DLPC) / Hu Kai, Jianwei Niu, Jianping Hu // Proc. of the International Conference on Parallel and Distributed Processing Techniques and Applications, PDPTA 2000, (Las Vegas, Nevada, USA, June 24–29, 2000). – Las Vegas: CSREA Press, – 8 p.

60. Sharifi M. Power-efficient distributed scheduling of virtual machines using workload-aware consolidation techniques / M. Sharifi, H. Salimi, M. Najafzadeh // The Journal of Supercomputing. –Netherlands: Springer, 2011. – P. 1 – 21.

61. Білоконь І. Побудова динамічно реконфігурованої обчислювальної архітектури з використанням технологій віртуалізації / І. Білоконь, Д. Грязнов, С. Погорілий // Вісник Київського національного університету імені Тараса Шевченка. – (Серія «Радіофізика та електроніка»). – 2010. – Вип. 14. – С. 4 – 6.

62. Кельтон В., Лоу А. Имитационное моделирование. Классика CS.3-е изд.-СПб.:Питер;Киев:Издательская группа BHV, 2004. – 847 с., ил.

63. Лазарев Ю. Моделирование процессов и систем в MatLab. Учебный курс – СПб.:Питер; Киев: Издательская группа БХВ,2005. – 512 с.:ил.

64. Морозов В.К., Рогачев Г.Н. Моделирование информационных и динамических систем М.: Издательский центр “Академия”, 2011. – 384 с.

65. Семеняка М.В. Исследование концепции иерархических очередей для решения задач управления перегрузками в телекоммуникационной сети / М.В. Семеняка, А.В. Симоненко // Сучасні інформаційно-комунікаційні технології (COMINFO'2012 – Livadia): VIII міжнар. наук.-техн. конф., 1-5 жовтня 2012 р.: зб. тез – К: ДУІКТ, 2012. – С. 68-70. 314

66. Lemeshko O. Researching and designing of the dynamic adaptive queue balancing method on telecommunication network routers / O. Lemeshko, M. Semenyaka, O. Simonenko // The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM'2013): XII international conference, 19-23 Febr. 2013. – Lviv: Lviv Polytechnic Publishing House, 2013. – P. 204-207.

67. Лемешко А.В. Модель активного управления очередями на маршрутизаторах телекоммуникационной сети / А.В. Лемешко, М.В. Семеняка, А.В. Симоненко // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – Ростов-на-Дону: ПЦ "Университет" СКФ МТУСИ'2015. – Ч.1 – С. 244-248.

68. Симоненко А.В. Математическая модель управления очередями на маршрутизаторах телекоммуникационной сети на основе оптимального агрегирования потоков и распределения пакетов по очередям [Електронний ресурс] / А.В. Симоненко, Д.В. Андрушко // Проблеми телекомунікацій. – 2015. – № 1 (16). – С. 94 - 102. – Режим доступу до журн.: http://pt.journal.kh.ua/2015/1/1/151_simonenko_queue.pdf.

69. Lemeshko O. Researching and designing of the dynamic adaptive queue balancing method on telecommunication network routers / O. Lemeshko, M. Semenyaka, O. Simonenko // The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM'2013): XII international conference, 19-23 Febr. 2013. – Lviv: Lviv Polytechnic Publishing House, 2013. – P. 204-207.

70. Червенець В. В. Підвищення якості передачі потокового трафіку в мультисервісних мережах : дисертація на здобуття наукового ступеня кандидата технічних наук : 05.12.02 – телекомунікаційні системи та мережі / Володимир Володимирович Червенець ; Міністерство освіти і науки України,

Національний університет "Львівська політехніка". – Львів, 2016. – 173 с. – Бібліографія: с. 151–166 (121 назва).