УДК 621.396.662

к.т.н. Бовда Е.М. (ВІТІ)
Плугова О.Б. (НЦЗІ)
Бондаренко В.Г. (ВІТІ)

МЕТОД ОБМЕЖЕННЯ ВХІДНОГО НАВАНТАЖЕННЯ В *SDN* МЕРЕЖАХ

В статті проведено огляд процедур щодо обмеження вхідного навантаження в SDN мережах, проведено аналіз сучасних підходів з обмежень вхідного навантаження, запропоновано підхід щодо обмеження вхідного навантаження в SDN мережах, в основу якого покладено метод обчислення пропускної здатності мережі.

Бовда Э.М., Плуговая О.Б., Бондаренко В.Г. Метод ограничения входной нагрузки в SDN сетях. *В статье проведен обзор процедур ограничения входящей нагрузки в SDN сетях, проведен анализ современных подходов по ограничению входящей нагрузки, предложен подход по ограничению входящей нагрузки в SDN сетях, в основу которого положен метод вычисления пропускной способности сети.*

E. Bovda, O. Plugova, V. Bondarenko The method of limiting the input load in SDN networks. *The article provides an overview of the procedures for limiting the incoming load in SDN networks, an analysis of modern approaches to limit the incoming load, an approach is proposed to limit the incoming load in SDN networks, which is based on the method of calculating the network capacity.*

Ключові слова: *управління доступом, управління потоками, управління трафіком, пропускна здатність мережі, обмеження вхідного навантаження, SDN мережа.*

Постановка проблеми в загальному вигляді. Завдання управління з обмежень вхідного навантаження мережі відноситься до виконання функції управління доступом зовнішніх потоків даних у мережу [1]. Ресурси мережі завжди є обмежені, тому коли зовнішні потоки даних перевищують допустимі значення, то виникають перенавантаження. Їх поява значно знижує характеристики якості повідомлень, що передаються в мережі, а також може привести до зменшення пропускної спроможності або блокування мережі.

Для попередження виникнення таких ситуацій в мережі повинен бути дієвий механізм обмежень доступу зовнішніх потоків даних для обмеження вхідного навантаження.

Аналіз останніх публікацій. В роботі [1] запропоновано підхід, де для організації управління доступом повідомлень у мережу використовується метод обчислення пропускної спроможності мережі з комутацією пакетів. При цьому визначається частина пакетів, що можуть бути прийняті на обслуговування мережею та будуть розподілені по маршрутах доставки; визначаються потоки, що можуть бути втрачені в процесі доставки; визначається загальна кількість повідомлень, що передана з завданою якістю.

В роботі [2] розглянуто *mesh*-мережі, де для ефективного управління використовуються два підходи до маршрутизації – проактивний (протокол *OLSR*) та реактивний (протокол *AODV*). *OLSR* дозволяє здійснювати збір та розповсюдження службової інформації про стан мережі. Як наслідок, кожний вузел може будувати модель поточного стану мережі у вигляді формального опису графа. Вузол може обчислити „довжину" найкоротших шляхів до всіх адресатів у мережі і вибрати „оптимальний" маршрут, що веде до будь-якого окремого вузла мережі. *AODV* передбачає пошук і організацію маршрутів по мірі їх необхідності, а також руйнування знайдених маршрутів після їх використання. Дані протоколи є статичні по відношенню до зовнішнього трафіка та перерозподілу навантаження. В роботі [3] одним із завдань є управління потоками, яке спрямоване на обмеження вхідного та транзитного навантаження в мережі. Для цього використовується управління обсягом переданих по мережі потоків і управління розподілом на мережі потоків. Управління обсягом переданих по мережі потоків можна здійснити шляхом управління обмеженням вихідного навантаження, а управління розподілом на мережі потоків – перерозподілом шляхів передачі потоків та визначенням числа допустимих обхідних шляхів. В роботі [4] обгрунтована ефективність застосування технології програмного конфігурування для адаптивного управління трафіком *SDN* мереж. Експериментами доведено, що запропоновані рішення найбільш ефективні при високому навантаженні каналів передачі даних, що дає потрібний баланс між показниками пропускної здатності та затримок пакетів. В роботі [5] розглянуто переваги використання технології *SDN* мереж, які полягають в підвищенні ефективності

використання пропускної здатності каналів, балансуванні навантажень у мережі; спрощенні управління мережею, підвищенні масштабованості мережі; підвищенні безпеки мереж; створенні ефективної маршрутизації; зниженні капітальних витрат. Розглянуто способи реалізації даного підходу: на базі віртуальних комутаторів за технологією *Overlay*; на базі серверів агрегації трафіка; на базі спеціальних комутаторів. Наведено переваги та недоліки кожного зі способів реалізації. Вказано, що реалізація цих способів обумовлюється вимогами до експлуатації та ефективності роботи *SDN* мереж.

В роботі [6] розглянута потокова модель адаптивної маршрутизації для програмно-конфігурованих мереж з балансуванням навантаження за критеріями оптимальності процесу балансування навантаження, який пов'язаний з роботою мережі в цілому і зводився до мінімізації коефіцієнта максимального завантаження каналів телекомунікаційної мережі та критерія адаптації процесу балансування навантаження, виконання якого пов'язане із забезпеченням рівності нулю контурних затримок пакетів для кожного трафіка окремо. В результаті дослідження встановлено, що використання запропонованої моделі дозволяє поліпшити середню багатошляхову затримку пакетів від 10 – 16 до 35 – 39 %, а також ймовірність своєчасної доставки на 17 – 63 % в порівнянні з раніше відомими моделями маршрутизації. При цьому гарантується рівність середніх затримок уздовж множини шляхів, які розраховуються, що сприяє мінімізації джиттера пакетів, який обумовлений реалізацією багатошляхової стратегії маршрутизації. В роботі [7] показано *SDN* архітектуру, яка складається з трьох рівнів: інфраструктурного, управління та мережевих додатків. Розглянуто *OpenFlow* стандарт, завдяки якому надається доступ та зв'язок між рівнями управління та архітектури, а також принцип роботи комутатора та контролера *SDN* мережі. *OpenFlow* дозволяє запрограмувати мережу для різних оптимізацій на основі кожного потоку. Крім того, *OpenFlow* пристрій здатний переписувати пакети, тобто він може діяти як *NAT* або *AFTR* (*Address Family Transition Router*). Оскільки він може відкидати пакети, то пристрій здатний діяти як брандмауер. Він також може реалізувати *ECMP* (*equal-cost multi-path*) або інші алгоритми балансування навантаження. Маршрутизатор може мати різні правила для різних потоків, що проходять через них. Він може розподіляти навантаження для одного потоку, використовувати брандмауер для іншого і змінювати заголовки пакетів для третього потоку. *SDN* технологія може використовуватися для віртуалізації мереж з метою більш ефективного використання мережевих ресурсів. Таким чином, окремі елементи мережі стають значно більш гнучкими в умовах *OpenFlow* в порівнянні з традиційною мережею. В роботі [8] розглянуто гібридна модель *SDN* мережі на основі протоколу маршрутизації *EIGRP*. Маршрутизатори обмінюваються префіксами, що знаходяться в їх таблицах: IP адреса мережі, маска підмережі, полоса пропускання мережі, затримка на інтерфейсі маршрутизатора та інш. На основі цієї інформації маршрутизатор розраховує стандартну або розширену метрики. Кожна зміна метрики породжує дифузійне обчислення метрик та маршрутів іншими маршрутизаторами, що призводить до частих змін маршрутів та нестабільності мережі. Запропоновано використати адаптивний алгоритм реагування на зміни навантаження, який рекомендовано використовувати в гібридній *SDN* мережі. Це дозволить забезпечити більший управляючий контроль над мережею та попередить відмови в обслуговуванні. На основі проведеного аналізу маємо зробити висновок, що переважна більшість вище наведених авторів проводили свої дослідження з управління обмеженнями доступу потоків в мережі, де в неповній мірі враховуються характеристики, що вимірюються за певний період часу, а це призводить до неефективного використання пропускної здатності ліній зв'язку.

Метою статті є створення методу обмеження вхідного навантаження в *SDN* мережах при забезпеченні оптимізації ресурсів пропускної здатності мережі.

Виклад основного матеріалу. В основу функціонування *SDN* мереж покладено наступні ідеї: поділ процесів передачі та управління даними; єдиний, уніфікований, інтерфейс між рівнем управління і рівнем передачі даних; логічно централізоване управління

мережею, що здійснюється за допомогою контролера з встановленої мережевою операційною системою і мережевими додатками; віртуалізація фізичних ресурсів мережі.

Мережа (рис. 1) складається з контролера та комутаторів *SDN* (пристрої), а також звичайних комутаторів (маршрутизаторів). Контролер є центральною ланкою, що визначає роботу всієї мережі як по передачі даних так організації мережевої безпеки. На контролері визначається політика управління мережею на основі заданих правил, а також роботи спеціалізованих додатків. Управляючі впливи передаються на комутатори по протоколу *OpenFlow* у вигляді *flow*-таблиць, що містять інформацію про те, куди, як і який трафік передавати. Такий підхід дає велику гнучкість в управлінні мережею і істотно спрощує адміністрування (а також архітектуру) мережі. Система мережевої безпеки на базі *OpenFlow*, що реалізується на контролері централізує цю функцію і забирає на себе весь інтелект *firewall*-ів, *IPS*-ів та інших традиційних систем мережевого захисту.

Пристрій *OpenFlow* складається з трьох компонент: таблиці потоків (англ. *flow table*); безпечного каналу (англ. *secure channel*), що використовується для управління комутатором зовнішнім „інтелектуальним" пристроєм (контролером); протоколу *OpenFlow protocol*, що використовується для управління.

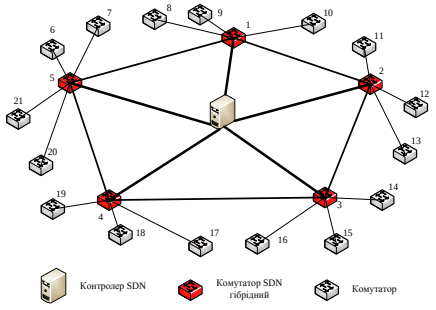

Рис. 1 Приклад використання гібридних комутаторів на межах SDN мережі

Згідно зі специфікацією 1.3 стандарту *OpenFlow* [6 – 10], взаємодія контролера з комутатором здійснюється за допомогою протоколу *OpenFlow* – кожен комутатор повинен містити одну або більше таблиць потоків (*flow tables*), групову таблицю (*group table*) і підтримувати канал (*OpenFlow channel – secure channel*) для зв'язку з контролером. Кожна таблиця потоків в комутаторі містить набір записів (*flow entries*) про потоки або правила. Кожний такий запис складається з полів-ознак (*match fields*), лічильників (*counters*) і набору інструкцій (*instructions*). Механізм роботи комутатора *OpenFlow* полягає в наступному: у кожного пакета, що прийшов „вирізується" заголовок (бітовий рядок певної довжини). Для цього бітового рядку в таблицях потоків, починаючи з першого, шукається правило. Знайдене правило повинно найближче відповідати заголовку пакета. При наявності збігу, над пакетом і його заголовком виконуються перетворення, які визначаються набором інструкцій, зазначених в знайденому правилі. Інструкції, що асоційовані з кожним записом таблиці, описують дії, пов'язані з пересилкою пакета, модифікацією його заголовка, обробкою в таблиці груп, обробкою в конвеєрі і пересиланням пакета на певний порт комутатора. Інструкції конвеєра обробки дозволяють пересилати пакети в наступні таблиці для подальшої обробки та у вигляді метаданих передавати інформацію між таблицями. Інструкції також визначають правила модифікації лічильників, які можуть бути використані **для збору різноманітної статистики**. Якщо потрібного правила в першій таблиці не виявлено, то пакет інкапсулюється і відправляється контролеру, який формує відповідне правило для пакетів даного типу і встановлює його на комутаторі (або на наборі керованих їм комутаторів), або пакет може бути скинутий (в залежності від конфігурації комутатора). Запис про потік може наказувати пересилання пакета в певний порт (звичайний фізичний порт або віртуальний, призначений комутатором, або зарезервований віртуальний порт, встановлений специфікацією протоколу). Зарезервовані віртуальні порти можуть визначати загальні дії пересилання: відправка контролера, лавинна розсилка, пересилання без

OpenFlow. Віртуальні порти, що визначені комутатором, можуть точно визначати групи агрегування каналів, тунелі або інтерфейси зі зворотним зв'язком. Записи про потоки можуть також вказувати на групи, в яких визначається додаткова обробка. Групи є наборами дій для широкомовної розсилки, а також набори дій пересилання з більш складною семантикою, наприклад, швидка зміна маршруту або агрегування каналів. Механізм груп дозволяє ефективно змінювати загальні вихідні дії для потоків. Таблиця груп містить записи про групи, що містять список контейнерів дій зі спеціальною семантикою, що залежить від типу групи. Дії в одному або декількох контейнерах дій застосовуються до пакетів, що відправляються в групу. Установка, оновлення та видалення правил в таблицях потоків комутатора здійснюються контролером. Правила можуть встановлюватися реактивно (у відповідь на пакети, що прийшли) або проактивно (заздалегідь, до приходу пакетів).

Контролер може керувати як одним, так і кількома *OpenFlow*-комутаторами і містить мережеву операційну систему, яка надає мережеві сервіси по низкорівневому управлінні мережею, сегментами мережі і станом мережевих елементів, а також додатки, які здійснюють високорівневе управління мережею і потоками даних. Звичайні комутатори (маршрутизатори) не управляються контролером, але можуть бути їм використані для збору статистичних характеристик про потоки, які проходять через них. Контролер використовує цю інформацію для аналізу ситуацій, що складуються, а також видачі управляючих впливів на *SDN* комутатори. Мережева ОС (МОС) забезпечує додаткам доступ до управління мережею і постійно відстежує конфігурацію засобів мережі. Під МОС розуміється програмна система, що забезпечує моніторинг, доступ і управління ресурсами всієї мережі, а не її конкретного вузла [9]. МОС забезпечує програмний інтерфейс для додатків управління мережею і реалізує механізми управління таблицями комутаторів: додавання, видалення, модифікацію правил і збір різноманітної статистики. Таким чином, фактично рішення задач управління мережею виконується за допомогою додатків, реалізованих на основі *API* мережевої операційної системи, що дозволяють створювати додатки в термінах високорівневих абстракцій (наприклад, ім'я користувача та ім'я хоста), а не низькорівневих параметрів конфігурації (наприклад, *IP*- і *MAC* адрес). Це дозволяє виконувати керуючі команди незалежно від базової топології мережі, але вимагає, щоб МОС підтримувала відображення між високорівневими абстракціями і низькорівневими конфігураціями. У кожному контролері є хоча б один додаток, який управляє комутаторами, з'єднаними з цим контролером, і формує уявлення про топології фізичної мережі, що знаходиться під управлінням контролера, тим самим централізуючи управління. Подання топології мережі включає в себе топологію комутаторів, розташування користувачів та хостів і інших елементів та сервісів мережі. Подання також включає в себе прив'язку між іменами та адресами, тому одним з найважливіших завдань, що вирішуються МОС, є постійний моніторинг мережі [7 – 10]. Для контролерів в *SDN* дуже важливим є вимога того, що всі програми одного контролера в кожен момент часу повинні мати однакове уявлення про топологію мережі. *SDN* мережі можуть реалізовувати механізм віртуалізації [9, 10]. Під віртуалізацією мережі розуміється ізоляція мережевого трафіка – групування (мультиплексування) декількох потоків даних з різними характеристиками в рамках однієї логічної мережі, яка може розділяти єдину фізичну мережу з іншими логічними мережами або мережевими зрізами (*network slices*). Кожен такий зріз може використовувати свою адресацію, свої алгоритми маршрутизації, управління якістю сервісів та інш.

Віртуалізація мережі дозволяє: підвищити ефективність розподілу мережевих ресурсів і збалансувати навантаження на них; ізолювати потоки різних користувачів і додатків в рамках однієї фізичної мережі; адміністраторам різних зрізів використовувати свої політики маршрутизації і правила управління потоками даних; проводити експерименти в мережі, використовуючи реальну фізичну мережеву інфраструктуру; використовувати в кожному зрізі тільки ті сервіси, які необхідні конкретним додатків. **Представимо формалізовану постановку та рішення завдання.** *Дано*: $G=(V, E)$ – мережа, де V – множина вузлів мережі

V={υ_1,… υ_n}, а E – множина спрямованих ліній зв'язків E={ $e_1, \dots, e_m$}$\in V \times V$; b_{uv} – пропускна здатність спрямованого зв'язку; ρ_{uv} – коефіцієнт навантаження лінії зв'язку; $\Lambda = \sum_{r=1}^{R} \lambda_r$ – потік пакетів з інтенсивністю λ, де r – номер пріоритетного потоку $r = 1, R$; набір $\underline{D} = \{\underline{D}_1, \underline{D}_2, \dots, \underline{D}_k\}$ потоків K повинен бути маршрутизований через мережу, де кожен потік κ представляється як кортеж $\underline{D}_k$ = (h_k, t_k, T_k, P^k_p), де параметри h_k і t_k є вузел-джерело для потоку k і вузел призначення для потоку k; $T_k = (t_{ij}) \in R^{n \times n}$ – трафік, який необхідно передати між вузлами мережі, де кожний елемент t_{ij} відповідає трафіку, що необхідно передати від вузла υ_i до вузла υ_j; P^k_p – множина допустимих шляхів між h і t; змінна x_{uv}^{kp} – зв'язок (u, v), що належить p-му шляху, який використовується для маршрутизації потоків κ джерела до місця призначення; змінна y_{uv}^{kp}, що вказує обсяг трафіка, що передається по ребру (u, v) для потоку κ на його p -й шлях; $q_Q^{kp} \in 0, \dots, Q$ – цілочисельна змінна, де поділ смуги пропускання T_k за p -й шлях здійснюється відповідно до співвідношення $\frac{q_Q^{kp}}{Q}$; θ – число правил, що знаходяться в таблицях потоків.

Припущення: Час оновлення таблиць динамічної маршрутизації не повинен перешкоджати доступу в мережу вхідного потоку пакетів. Кожен потік може бути передано кількома шляхами. Поділ потоку може бути виконано тільки на вході пристрою, використовуючи не більше P^k_p шляхів. Для кожного потоку в мережі повинні бути виконані умови збереження потоку:

$$\sum_{(h_k;v)\in E} x_{h_k v}^{kp} = 1, \quad \sum_{(u;h_k)\in E} x_{u h_k}^{kp} = 0, \tag{1}$$

$$\sum_{(t_k;v)\in E} x_{t_k v}^{kp} = 0, \quad \sum_{(u;t_k)\in E} x_{u t_k}^{kp} = 1, \tag{2}$$

$$\sum_{(u;v)\in E} x_{uv}^{kp} - \sum_{v;u \in E} x_{vu}^{kp} = 0, \ \forall u \in V \setminus h_k, t_k \ . \tag{3}$$

Обмеження (1), (2) та (3) по збереженню потоку, дозволяють спрямовувати трафік кожного потоку від свого вузла-джерела h_k до його вузла призначення t_k за P_p^k шляхом. Вони також запобігають циклам, що утворюються у джерела або цілі призначення. Вимога на розподіл потоку може бути передана через мережу тільки в тому випадку, якщо вона не перевищує пропускну здатність ліній зв'язку та відповідний коефіцієнт навантаження лінії зв'язку:

$$\sum_{k=1}^{K} \sum_{p=1}^{P_p^k} y_{ve}^{kp} \le b_{ve}, \text{або } \rho_{ve} = \sum_{k=1}^{K} \sum_{p=1}^{P_p^k} y_{ve}^{kp} / b_{ve} \le 1. \tag{4}$$

Частковий потік y_{ve}^{kp} (тобто, пропускну здатність, що призначена шляху p) обчислюється як добуток змінного шляху x_{ve}^{kp}, який вказує шлях p потоку k та використовує ребро (u,v) та частину потоку k, що виділений шляху p, а саме $T_k \sum_{Q=1}^{\theta} \frac{q_Q^{kp}}{Q}$.

$$y_{ve}^{kp} = T_k x_{ve}^{kp} \sum_{Q=1}^{\theta} \frac{q_Q^{kp}}{Q} \tag{5}$$

Потрібно: знайти оптимальне рішення з обмеження вхідного навантаження в *SDN* мережі з метою оптимізації ресурсів пропускної здатності мережі.

Метод обмеження вхідного навантаження в SDN мережах.

Розрізняють наступні процедури управління доступом: локальне, міжкінцеве та глобальне управління зовнішніми потоками. Суттю локального управління є відключення зовнішніх джерел при погрозі переповнення пам'яті маршрутизатора (комутатора). Можливий варіант вибіркового відключення джерела на основі статистичного аналізу характеристик потоків. Локальне управління, таким чином, захищає мережу від захвату ресурсів одних джерел на шкоду іншим. Міжкінцеве управління забезпечує обмеження загального числа пакетів, що знаходиться в мережі за рахунок блокування джерел, які видали в мережу визначено число пакетів, але не отримали жодного підтвердження від одержувача. Допустиме число пакетів між парами джерело-одержувач може варіюватися в залежності від

ресурсів продуктивності каналів та маршрутизаторів (комутаторів). Глобальне управління (ізаритмічний метод) забезпечує обмеження загального числа пакетів в мережі завдяки циркуляції по мережі деякого числа дозволів – спеціальних службових повідомлень. Джерело не може увести пакет в мережу поки не отримає на це дозвіл. Процедури управління доступом можуть негативно взаємодіяти з процедурами маршрутизації [1, 6, 10], тому необхідно передбачити введення обґрунтованого обмеження на величину вхідного в мережу потоку пакетів, пропускаючи в мережу потоки, при яких для процедури маршрутизації забезпечується допустимий час доведення службових управляючих повідомлень. Суть методу управління доступом для всієї мережі полягає в тому, що в процесі управління обчислюються пропускні здатності елементів мережі, з урахуванням яких відбувається перерозподіл потоків повідомлень та прийом на обслуговування такої кількості нових повідомлень при забезпеченні потрібної якості їх обслуговування та виконанні обмеження на те, що маршрутизація виконується таким чином, щоб максимально забезпечити пропускну здатність елементів мережі.

Управління доступом передбачає виконання наступних операцій:

1. Визначення максимальних інтенсивностей потоків λ_r, які можуть бути обслуговані з потрібною якістю.

2. Обчислення частки потоків $\lambda_r^{\text{втр}}$, які можуть бути втрачені в процесі передачі по мережі.

3. Винайдення частки додаткових потоків $\lambda_{r_{\text{дод}}}^{ht}$, що генеруються транспортним рівнем при поновленні пакетів:

$$\lambda_{r_{\text{дод}}}^{ht} = \lambda_{r_{\text{втр}}}^{ht} * P_r^{ht}(1 + \ 1 - P_r^{ht} \ + \cdots + \ 1 - P_r^{ht} \ ^k,$$

де $P_r^{ht} \ -$ ймовірність своєчасного обслуговування пакетів r пріоритету при передачі їх від h до t через мережу;

k – число повторних передач пакетів з транспортного рівня при їх втратах в мережі.

4. Обчислення значень порогів $Д_r^{ht}$ лічильника дозволів для фіксованого часу

$$Д_r^{ht} \ t \ = \lambda_r^{ht} - \lambda_{r_{\text{дод}}}^{ht}.$$

5. Розсилання знайдених значень порогів у всі інтерфейси.

6. Після виставлення порогів в інтерфейсах здійснюється отримання службових донесень про виставлені порогові значення, прогнозовані значення інтенсивностей вхідних зовнішніх потоків та зміни в структурі мережі.

7. При зміні ситуації в мережі необхідно провести обчислення порогових значень на новий момент часу. Для організації управління доступом повідомлень в мережу використовується метод обчислення пропускної здатності мережі, який складається з трьох етапів: визначення частки потоків, які можуть бути прийняті на обслуговування мережею та розподіл їх по шляхам доставки; визначення потоків, що втрачені в процесі їх передавання; визначення загальної кількості повідомлень з потрібною якістю. На першому етапі вирішується оптимізаційне завдання: для кожного з пріоритетних потоків λ_r необхідно знайти такі λ_t^+, при яких досягається максимум добутку коефіцієнтів недовикористання пропускних здатностей каналів зв'язку:

$$\lambda_t^+ = \max_{\lambda_{ver}^{kp} \in \lambda_r} \quad _{i \in N} \quad _{j \in N}(1 - \frac{c_{ij} + \lambda_{ij(r-1)} + \ _{k=1}^{N} \ _{j=1}^{N} \lambda_{ijr}^{kp}}{K_{\text{г}ij}\mu_{ij}}), \tag{6}$$

де λ_{ijr}^{kp} – пріоритетний потік, що передається по каналу зв'язку; c_{ij} – потік службової інформації; $K_{\text{г}ij}$ – коефіцієнт готовності каналів зв'язку; λ_{ver}^{kp} та $\lambda_{ij(r-1)}$ – інтенсивності потоків між вузлами та каналами зв'язку; μ_{ij} – інтенсивність обслуговування вканалі зв'язку.

Для рішення завдання (6) можливо використати ітеративний алгоритм, який полягає в тому, що спочатку фіксується потік з найвищим пріоритетом, а потім виконуються наступна послідовність дій:

1. Проводиться ранжування потоків пріоритету, який обрано та обирається перший з них.

2. Для обраного потоку знаходяться всі шляхи та проводиться їх ранжування по критерію максимальної пропускної здатності.

3. Потік спрямовується по шляху з максимальною пропускною здатністю. З мережі віднімається ця частина пропускної здатності, яка задіяна для передавання потоку.

4. Обирається наступний за рангом потік та виконуються п. 2, 3. Якщо всі потоки розподілено, то перехід на наступний крок.

5. Обчислюється значення цільової функції $F(1)$ у виразі (6).

6. Обирається потік, що має мінімальний ранг.

7. Деяка частина обраного потоку $\Delta\lambda^{kp}$ спрямовується по першому обхідному шляху.

8. Якщо навантаження на цьому шляху перевищує порогове значення для цього пріоритету, то цей шлях виключається з розгляду. Перехід до виконання кроку 9, в противному випадку переходимо до кроку 9.

9. Обчислюється нове значення цільової функції $F(2)$ за виразом (6). Якщо $F(2)>F(1)$, то $F(1)$ присвоюється значення $F(2)$ й розподіл потоку приймається, в противному випадку значення $F(1)$ не змінюється та розподіл не приймається.

10. Обирається наступний обхідний шлях та по ньому спрямовується $\Delta\lambda^{kp}$. Перехід до кроку 7. Повторення кроків 7 – 9 поки всі обхідні шляхи не будуть розглянуті.

11. З нерозподіленого потоку, що залишився береться нова частка $\Delta\lambda^{kp}$ та виконується крок 7. Крок 10 виконується до тих пір, поки не вичерпається потік.

12. Після того, як буде розподілено всі потоки старшого пріоритету, обчислюються нові значення для потоків меншого пріоритету. Як результат отримуємо сумарні потоки на вході каналу зв'язку з урахуванням маршрутизації, управління потоками та пріоритету їх обслуговування. На другому етапі визначимо втрати пакетів при передаванні інформації та можливого блокування на вузлах. Для цього використовують модель багатоканального тракту передачі даних з різнотипними каналами. Тоді ймовірність своєчасного передавання пакетів r пріоритету через канал зв'язку:

$$P_r = \sum_{u=0}^{b} P_r(H_u) \cdot P_r(A \mid H_u), \tag{7}$$

де $P_r(H_u)$ – ймовірність гіпотези H_u, що полягає в безвідмовній роботі каналу зв'язку; $P_r(A \mid H_u)$ – умовна ймовірність події A, що складається в обслуговуванні пакету при виконанні гіпотези H_u. Для визначення $P_r(H_u)$ та $P_r(A \mid H_u)$ використовуються методи теорії масового обслуговування [1]. Тоді ймовірність $P_r(H_u)$ для неоднорідних каналів визначається за схемою Бернулі:

$$P_r(H_u) = \sum_{k=0}^{C_b^u} \prod_{i \in k} P_{ri} \prod_{j \in (b-k)} (1 - P_{ij}), i \neq j. \tag{8}$$

Умовна ймовірність обслуговування пакетів $P_r(A \mid H_u)$ це ймовірність обслуговування потоків в u канальній системі масового обслуговування з чергою обмеженої довжини Q та обмеженим часом чекання в черзі:

$$P_r(A \mid H_u) = 1 - \frac{\frac{\delta_r \rho_r}{u!} \sum_{l=1}^{Q_r} l \frac{\rho_t^l}{\prod_{l=1}^{l}(u - i\delta_r)}}{1 + \sum_{k=0}^{u} \frac{\rho_r^k}{k!} + \frac{\rho_r^k}{u!} \sum_{l=1}^{Q_r} \rho_r^l \left(\prod_{i=1}^{l} \frac{\rho_r^l}{\prod_{l=1}^{l}(u - i\delta_r)} \right)}, \tag{9}$$

Підставляючи (8) та (9) в (7) отримуємо:

$$P_r = \sum_{u=1}^{b} P_{ru} \sum_{k=0}^{C_b^u} \prod_{i \in k} P_{ri} \prod_{j \in (b-k)} (1 - P_{rj}) \tag{10}$$

Ймовірність доведення пакетів за шляхом:

$$P_{\gamma r} = \sum_{\beta=1}^{w} P_{\beta r}, \tag{11}$$

де w – кількість каналів по шляху γ. При передаванні потоку за декількома шляхами імовірність доведення пакетів можна визначити за формулою:

$$P_{klr} = 1 - \prod_{\gamma=1}^{\pi} 1 - P_{\gamma r} \ , \tag{12}$$

де π – число шляхів передачі завданого потоку.

На третьому етапі визначаємо потік, що обслуговано:

$$\lambda_{klr}^{\text{обс}} = \lambda_{klr} \cdot P_{klr}, \ \ \lambda_{klr} \in \Lambda_r. \tag{13}$$

Кількість повідомлень, що передається в одиницю часу, визначається за формулою:

$$\Lambda_{\text{обс}} = \sum_{r=1}^{R} \sum_{k=1}^{N} \sum_{l=1}^{N} \frac{\lambda_{klr}^{\text{обс}}}{S_r}. \tag{14}$$

$\Lambda_{\text{обс}}$ якраз характеризує пропускну здатність мережі.

Висновок. У даній роботі було розглянуто рішення задачі обмеження вхідного навантаження мережі в системах управління з використанням *SDN* елементів для управління мережею. Отримана математична модель обмеження вхідного навантаження мережі, де використовуються *SDN* елементи та звичайні маршрутизатори. В якості цільової функції вибрана добуток коефіцієнтів недовикористання пропускних здатностей каналів зв'язку в мережі. Представлено формулювання задачі обмеження вхідного навантаження та забезпечення ефективної маршрутизації потоків повідомлень. Подальші дослідження будуть направлені на сумісне використання архітектури *SDN* мереж та підходів до ідентифікації станів системи, інтелектуалізації роботи *SDN* контролерів для ефективного управління телекомунікаційними мережами.

ЛІТЕРАТУРА

1. Арипов М. Н. Контроль и управление в сетях передачи данных с коммутацией пакетов / М. Н. Арипов, С. П. Присяжнюк, Р. А. Шарифов. – Ташкент: Фан, 1988. – 160 с.

2. SDN: новые возможности управления потоками в mesh – сетях. [електроний ресурс]. – режим доступу: https://habrahabr.ru/post/239649.

3. Управление системами связи специального назначения. [електроний ресурс]. – режим доступу: http://referatwork.ru/upravlenie_sistemami_svyazi.html.

4. Сосенушкин С.Е. Адаптивное управление ресурсами информационно-телекоммуникационной сети на основе программного конфигурирования / Сосенушкин С.Е., Круглова П.А. – Московский государственный технологический университет „СТАНКИН", Механика и машиностроение, 2015. – 479 – 484 с.

5. Смелянский Р.Л. Технологии *SDN* и *NFV*: новые возможности для телекоммуникаций. [електроний ресурс]. – режим доступу: http://arccn.ru/media/1132.

6. Лемешко А.В. Разработка и исследование потоковой модели адаптивной маршрутизации в программно-конфигурируемых сетях с балансировкой нагрузки / А.В. Лемешко, Т.В. Вавенко. – Управление, вычислительная техника и інформатика, Доклады ТУСУРа, № 3 (29), 2013. – 100 – 108 с.

7. Коломеец А. Е. Программно-конфигурируемые сети на базе протокола OpenFlow / [електроний ресурс]. – режим доступу: http://engbul.bmstu.ru/doc/711486.html.

8. Красов А.В. Метод управления трафиком в программно-определяемой сети / А.В. Красов, М.В. Левин, А.Ю. Цветков. – Информационные технологии и телекоммуникации. 2016. – Т. 4. № 2. – 53 – 63 с.

9. Отчёт о научно-исследовательской работе „Создание прототипа отечественной ПКС платформы управления сетевыми ресурсами и потоками с помощью сетевой операционной системы (СОС) на основе анализа и оценки существующих операционных систем для ПКС сетей и выбора одной из них для последующего развития по критериям производительности, масштабируемости, надёжности, безопасности" / Московский государственный универсистет имени М.В. Ломоносова, 2013.

10. Дорт-Гольц А.А. Разработка и исследование метода балансировки трафика в пакетних сетях святи: дис. на соискание ученой степени кандидата технических наук: 05.12.13 / Дорт-Гольц Антон Александрович. – Санкт-Петербург, 2014. – 168 с.