УДК 004.051 DOI: 10.31673/2786-8362.2024.028036

Гніденко М.П., к.т.н.; **Гніденко М.М.,**
Вишнівський О.В., Зінченко В.В.

ЗАБЕЗПЕЧЕННЯ ЕНЕРГОЕФЕКТИВНОСТІ ПРОГРАМНО ВИЗНАЧЕНИХ МЕРЕЖ (SDNs) ПРИ ВПРОВАДЖЕННІ РІЗНИХ СХЕМ БЕЗПЕКИ

Hnidenko M.P., Hnidenko M.M., Vyshnivskyi O.V., Zinchenko V.V. Ensuring the energy efficiency of Software Defined Networks (SDNs) when implementing various security schemes. Due to the ease of modifying network operations and adapting various energy efficient mechanisms, SDN provides a better solution not only for network security, but also for network ecology, which has become important in network design and deployment for economic and environmental benefits. Security schemes in place consume more power than without security schemes because security schemes consist of computations and communications that consume more power in the network. Therefore, a comprehensive study of both security and energy efficiency, as well as their compromise, is necessary. Data were collected to evaluate and compare the performance of an SDN network and a traditional network, and to study the trade-off between energy efficiency and security. Implementing some power-saving strategies in SDN can reduce overall power consumption, resulting in lower costs. The openness, ease, and programmability of SDN reduces the complexity of implementing energy efficiency approaches in both hardware and software. It would be more efficient to apply energy saving schemes in each module for overall energy saving. This requires knowing the power consumed in SDN by each module, such as chassis, routers, and nodes in the network. In addition, SDN is considered a viable solution where minimal resources can be used to perform a task without compromising overall network performance (e.g. security), thus reducing energy consumption. The choice of different SDN parameters depends on the applications that SDN is intended to support. For example, optimal SDN options may not be optimal SDN options for traditional data center networks, and optimal SDN options for IoT may not be optimal SDN options for cyber-physical systems. In this regard, it is necessary to always strive to achieve a compromise between safety and energy efficiency.

Keywords: Software-defined networks (SDNs), SDN controller, OpenFlow switch, energy efficiency

Гніденко М.П., Гніденко М.М., Вишнівський О.В., Зінченко В.В. Забезпечення енергоефективності програмно визначених мереж (SDNs) при впровадженні різних схем безпеки. Завдяки легкості модифікації мережевих операцій і адаптації різних енергоефективних механізмів, SDN забезпечує краще рішення не тільки для безпеки мережі, але й для екології мережі, яка стала важливою при проектуванні та розгортанні мережі для економічних і екологічних переваг. Запроваджені схеми безпеки споживають більше енергії, ніж без них, оскільки схеми безпеки складаються з обчислень і комунікацій, які споживають більше енергії в мережі. Тому необхідно комплексне дослідження як безпеки, так і енергоефективності, а також їх компроміс. Були зібрані дані для оцінки та порівняння продуктивності мережі SDN і традиційної мережі, а також для вивчення компромісу між енергоефективністю та безпекою. Впровадження деяких стратегій енергозбереження в SDN може зменшити загальне енергоспоживання.

Ключові слова: Програмно-визначені мережі (SDNs), контролер SDN, комутатор OpenFlow. енергоефективність.

Вступ

Програмно-визначені мережі (SDNs) з моменту їх появи демонструють свою перевагу у порівнянні з традиційними мережами у багатьох аспектах. Лише SDN надає інтелектуальний, адаптований, програмований та централізований дизайн мережі. SDN забезпечує програмування мережі, яка адаптується до програмних додатках в інтересах бізнеса та базується на основі відкритих стандартів. В той же час поведінка мереж SDN ще не до кінця вивчена і досліджена у різних умовах та обставинах, які виникають по мірі розширення сфери їх застосування. Важливо визначити, що SDN представляє собою насправді.

Постановка задачі. Ця стаття присвячена дослідженню переваг застосування SDN мереж у вирішенні екологічних проблем. Швидкий розвиток IT технологій приводить до стрімкого зростання енергоспоживання, що негативно відображається не лише на підвищенні накладних витрат експлуатації, а і на екологічному навантаженню на суспільство. Тому проблема енергоефективності IT надзвичайно актуальна у всіх аспектах їх застосування.

© Гніденко М.П., Гніденко М.М., Вишнівський О.В., Зінченко В.В. 2024

У даному випадку розглянемо проблему забезпечення енергоефективності мереж SDN при впровадженні різних схем безпеки

Аналіз останніх досліджень. Впровадження SDN мереж у даний момент є актуальною темою. Тому існує велика кількість досліджень щодо концептуальних підходів їх розвитку та розгортання у різних умовах [1,2,3], у тому числі забезпечення їх енергоефективності у різних умовах роботи [4], а також підвищення безпеки SDN мереж [5].

Метою роботи є забезпечення енергоефективності програмно визначених мереж (SDNs) при впровадженні різних схем безпеки. Варто зазначити, що запроваджені схеми безпеки споживають більше енергії, ніж без них, оскільки схеми безпеки складаються з обчислень і комунікацій, які споживають більше енергії в мережі. Тому необхідно комплексне дослідження як безпеки, так і енергоефективності, а також їх компроміс.

Виклад основного матеріалу дослідження.

Розглянемо різні підходи до енергозбереження в SDN, які показані на рисунку 1. Щоб побачити компроміс між енергоефективністю та мережевою безпекою, проаналізуємо та оцінюємо різні схеми безпеки, коли реалізовано SDN та технології енергозбереження.

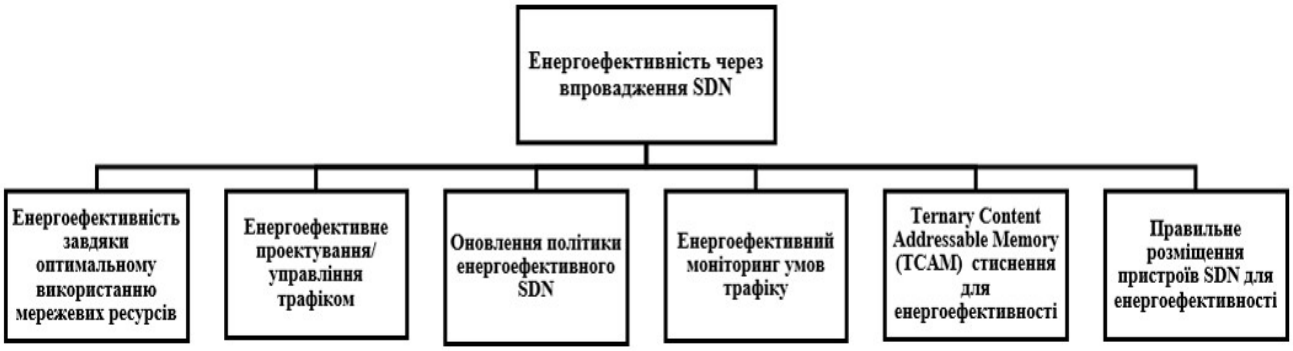

Рис. 1. Різні підходи до енергозбереження через впровадження SDN

Енергоефективність та її компроміс з безпекою в SDN. На рисунку 2 показаний невеликий тестовий стенд для SDN, де контролер OpenFlow відстежує загальний стан мережі. Комутатор OpenFlow пропонує сорок вісім портів 10/100/1000 Мбіт/с і чотири порти 1000/10000 Мбіт/с зі швидкістю комутації 176 Гбіт/с. Цей гібридний контролер підключає мережі OpenFlow до мереж L2/L3. Наявність доступу до цього комутатора зменшить складність мережі, усунувши потребу в традиційних мережевих протоколах завдяки підтримці OpenFlow 1.0 і 1.3.1. Технологія Virtual Tenant Networks (VTN) забезпечує безпечні мультитенантні хмарні мережі, які надають доступ до різноманітних уже існуючих пристроїв від інших третіх сторін. Крім того, була створена традиційна мережа, яка еквівалентна SDN, але мережеві функції були фіксовані, на відміну від SDN.

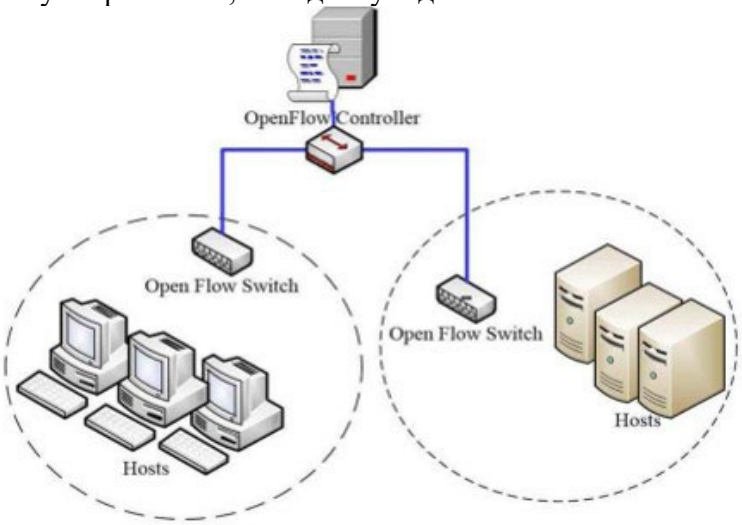

Рис. 2. Тестовий стенд мережі SDN на основі протоколу OpenFlow

Після цього були реалізовані різні схеми безпеки та схеми енергозбереження та були зібрані дані для оцінки та порівняння продуктивності мережі SDN і традиційної мережі, а також для вивчення компромісу між енергоефективністю та безпекою.

На рисунку 3 показаний графік порівняння споживання енергії з реалізацією SDN і без неї (адаптивна конфігурація як для безпеки, так і для енергоефективності) для шифрування та дешифрування одного файлу в різних симетричних шифрах і трансмутації цього файлу з одного комп'ютера на інший. На підставі аналізу даних, показаних на рисунку 3 можна зробити висновок, що споживання енергії для різних симетричних шифрів набагато вище в традиційній мережі, ніж у SDN. SDN споживає менше енергії (забезпечуючи однакову безпеку мережі) завдяки настроюваним функціям SDN, які дозволяють мережі регулювати як швидкість порту (оскільки порт 10 Мбіт/с споживає менше енергії, ніж порти 100 Мбіт/с або 1000 Мбіт/с), так і використання з'єднання за потребою, яка недоступна у традиційній мережі.

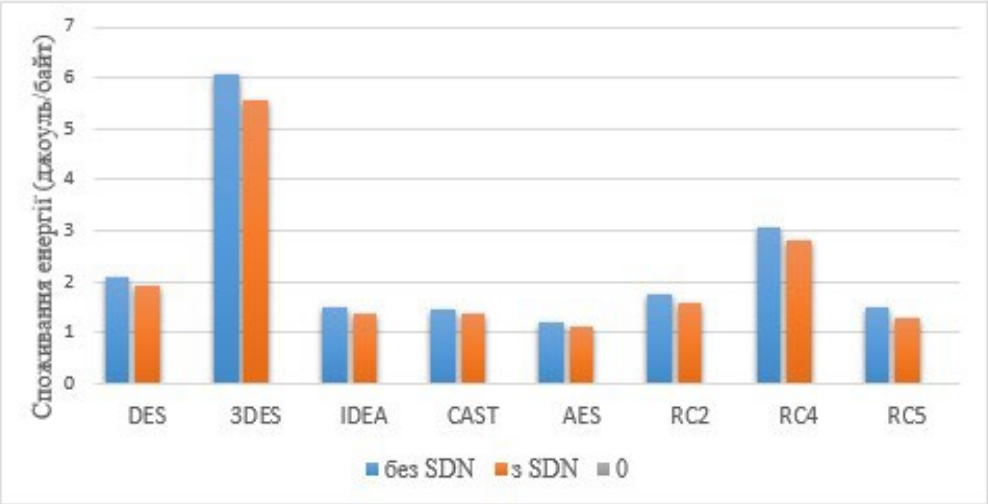

Рис. 3. Порівняння енергоспоживання з і без SDN при різних алгоритмах шифрування

Далі, був побудований графік зміни енергоспоживання для традиційної мережі та SDN для налаштування ключа в різних симетричних шифрах, як показано на рисунку 4. Під час обміну ключем SDN використовував низьку швидкість (наприклад, 10 Мбіт/с) без погіршення продуктивності мережі, оскільки розмір ключа невеликий. Але в традиційній мережі ключ невеликого розміру було замінено на високошвидкісне з'єднання, яке споживає більше енергії. Як наслідок, традиційна мережа споживає більше енергії порівняно з SDN, як показано на рисунку 4.

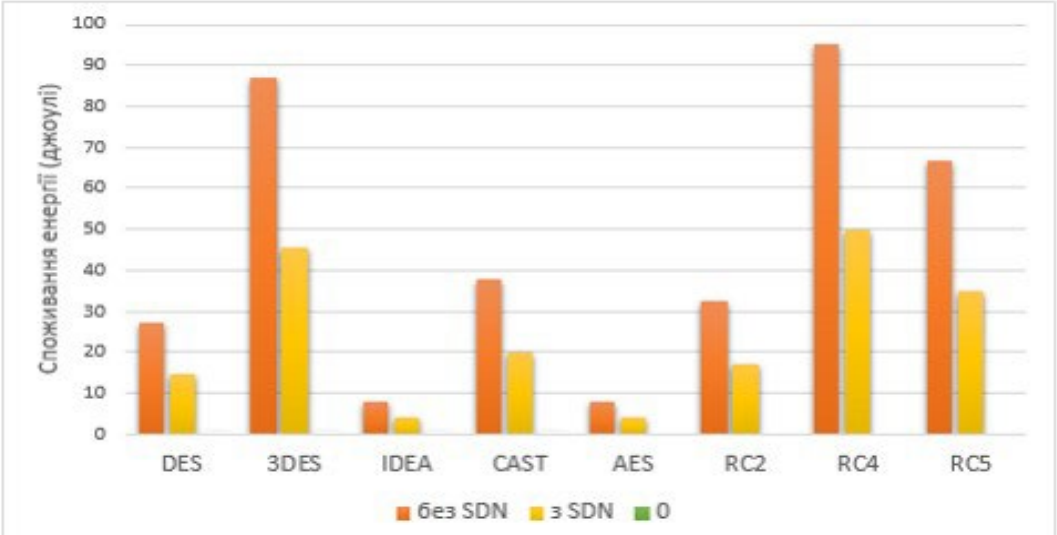

Рис. 4. Порівняння енергоспоживання з і без SDN при зміні ключа шифрування

На рисунку 5 показано графік зміни енергоспоживання з і без реалізації SDN для різних хеш-функцій для передачі одного файлу даних. Завдяки адаптивній природі SDN він регулює параметри мережі (швидкість порту/з'єднання, режим сну/увімкнення на основі активності з'єднання тощо) і споживає менше енергії, ніж у традиційній мережі.

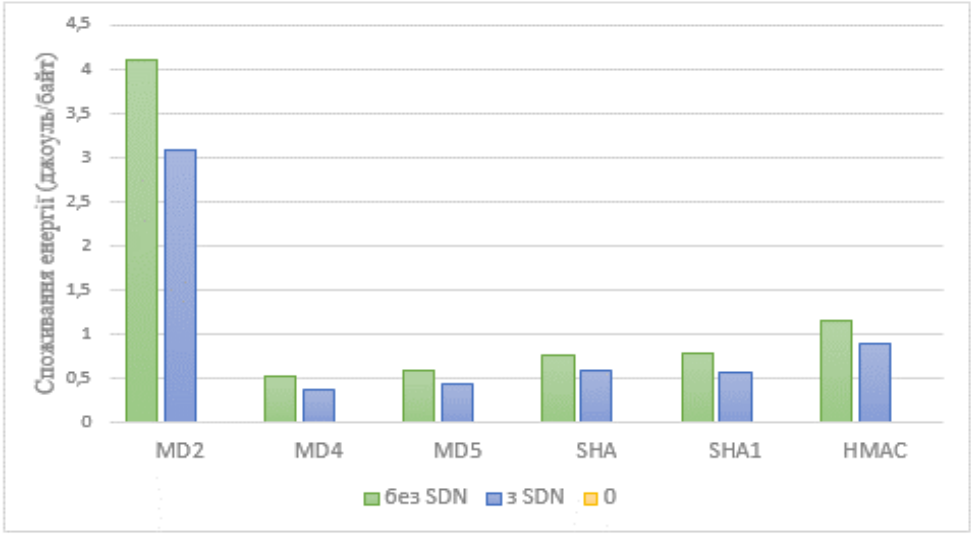

Рис. 5. Порівняння енергоспоживання з і без SDN для різних хеш функцій

Використовуючи результати досліджень, був побудований графік зміни енергоспоживання з і без реалізації SDN цифрових підписів для алгоритму цифрового підпису DSA (Digital Signature Algorithm) на рисунку 6 і для RSA (Rivest Shamir Adleman) на рисунку 7. Як у DSA, так і в RSA споживання енергії в традиційній мережі вище, ніж що в SDN.

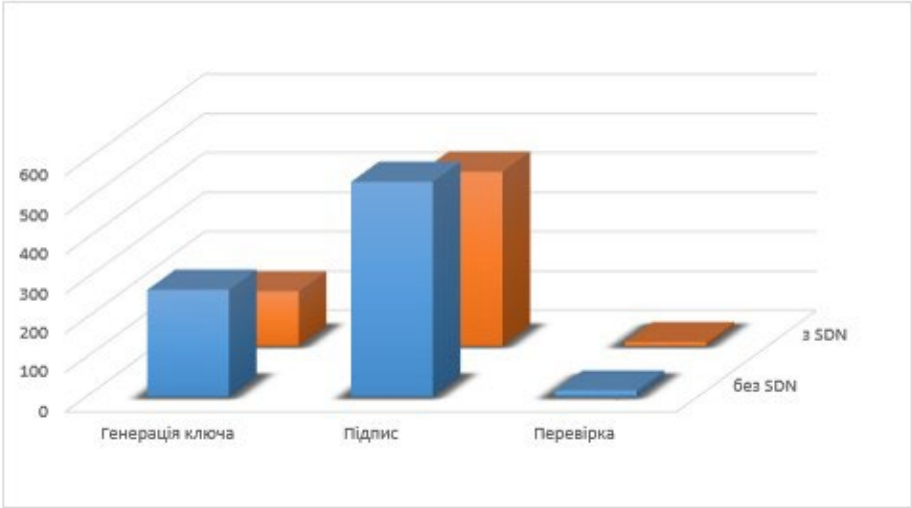

Рис. 6. Енергоспоживання для алгоритму цифрового підпису DSA

Була також реалізована схема безпеки RC5 у традиційній мережі та SDN для ідентичного експериментального налаштування. Графік варіації споживання енергії та безпеки для їх компромісу для шифрування RC5 і передачі інформації показано на рисунку 8. Як згадувалося раніше, SDN адаптує параметр зв'язку та робочі параметри, він споживає менше енергії, ніж традиційний мережі. Однак, коли SDN потребує вищого рівня безпеки (більше раундів для шифрування RC5 для кращої безпеки), споживання енергії зростає разом із рівнем безпеки (наприклад, кількістю раундів шифрування), як показано на рисунку 8.

Був побудований також графік зміни споживання енергії для рукоптискання рівня захищених сокетів (SSL) у традиційній мережі та в SDN зі збільшенням розміру даних, як показано на рисунку 9. Помітно, що споживання енергії збільшується зі збільшенням розміру

даних для обох, традиційна мережа та SDN. Однак споживання енергії для SDN нижче, ніж для традиційної мережі, оскільки SDN адаптує швидкість з'єднання на основі інформації, що передається.

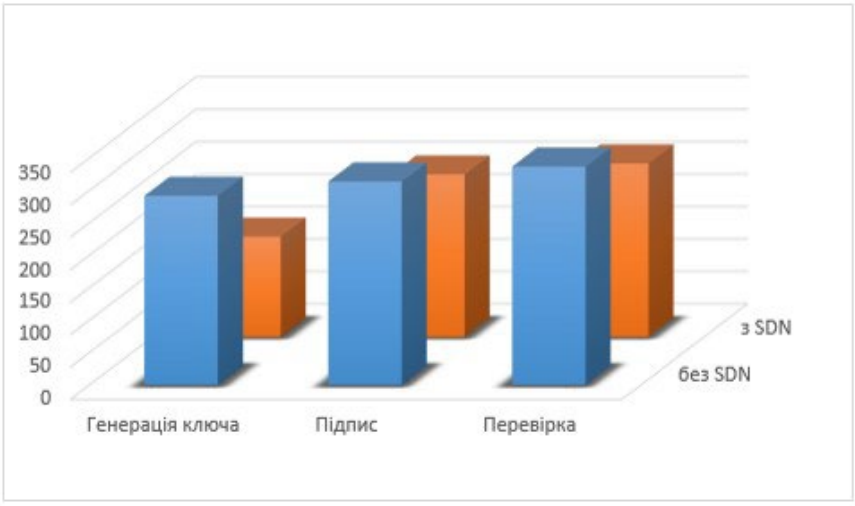

Рис. 7. Енергоспоживання для криптографічного алгоритму RSA

Рис. 8. Енергоспоживання для шифрування та передачі RC5

Коли SDN використовує свій максимальний ліміт швидкості та його канал використовується повністю, він споживає таку саму енергію, що й традиційна мережа, як показано на рисунку 10. Однак, коли є місце для використання нижчої швидкості зв'язку, він споживає менше енергії без погіршення продуктивності мережі.

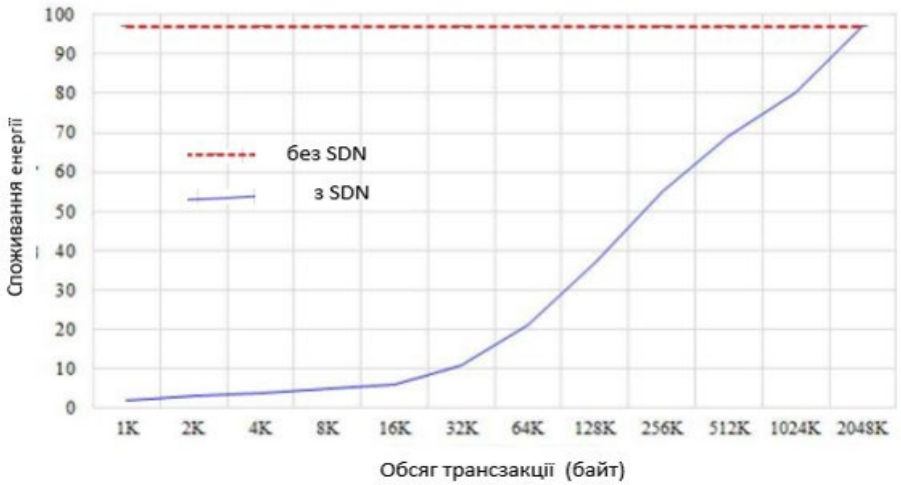

Рис. 9. Споживання енергії для SSL-рукопотискання зі збільшенням розмірів транзакцій

Нарешті, був побудований графік зміни середнього споживання енергії/потужності для традиційної мережі та SDN (з реалізацією безпеки/IPS і без неї), як показано на рисунку 10.

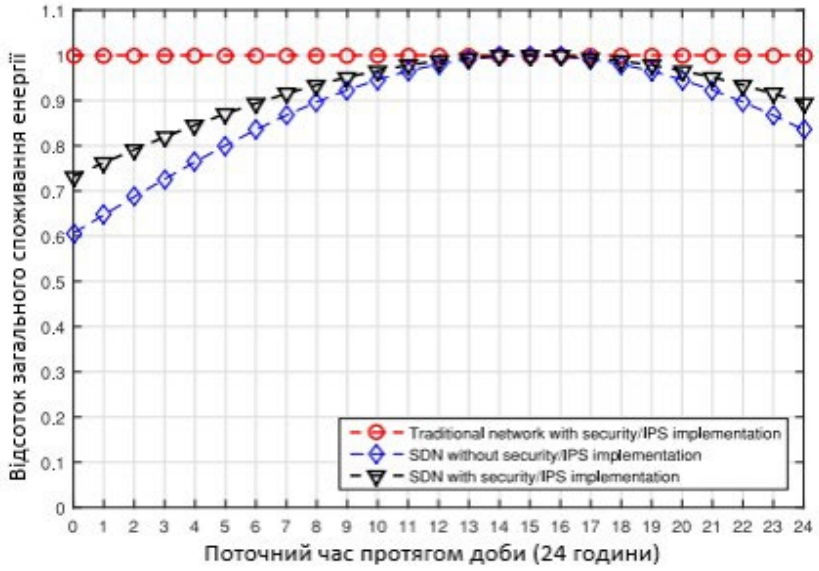

Рис. 10. Графік зміни середнього споживання енергії протягом доби

На рисунку 10 показана варіація відсотка середнього споживання енергії/потужності традиційною мережею та SDN з реалізацією безпеки/IPS і без неї для типового середовища домашнього офісу в малому офісі. Експеримент проводився в дослідницькій лабораторії з OpenFlow комутаторами та контролером, імітуючи шаблони трафіку комп'ютерної мережі університету.

У традиційній мережі, незалежно від часу, вона споживає однакову потужність, однак SDN споживає змінну потужність на основі навантаження, яка базується на часі доби, як показано на рисунку 10. У години пік вся мережа споживає максимальну потужність, однак SDN споживає менше енергії у непікові години. Коли реалізовано таку схему безпеки, як IPS, SDN споживає більше енергії, ніж без впровадження безпеки, як показано на рисунку 10. Таким чином, ми можемо підсумувати, що безпека пов'язана з витратами і нам потрібно розглянути компроміс між енергоефективністю та безпеки.

Ми можемо зробити висновок, що SDN може адаптувати свої параметри мережі на льоту, щоб забезпечити безпеку з меншим споживанням енергії порівняно з традиційною мережею. Іншими словами, енергоефективні підходи для SDN можуть допомогти споживати менше електроенергії, забезпечуючи кращий або такий же рівень продуктивності та безпеки, ніж у (еквівалентній) традиційній мережі. Таким чином, важливо вивчити енергоефективні підходи до SDN, які будуть надавати бажану ефективність.

Однією з головних проблем, з якою стикаються багато компаній у всьому світі, є кількість енергії, споживаної мережами. Потреба в постійній доступності та її величезна архітектура призводять до високого споживання енергії мережею. Компанії сплачують значний відсоток свого доходу для живлення своїх мережевих інфраструктурних структур. Використання енергоефективних мереж, таких як SDN, розглядається як рішення для зменшення загального споживання електроенергії в мережі. Це спонукало деякі компанії включити SDN у свої мережі. Впровадження деяких стратегій енергозбереження в SDN може зменшити загальне енергоспоживання, що призводить до зниження витрат. Відкритість, легкість і програмованість SDN зменшує складність реалізації підходів енергоефективності як в апаратному, так і в програмному забезпеченні. Ефективніше було б застосувати схеми енергозбереження в кожному модулі для загального енергозбереження. Для цього потрібно знати потужність, споживану в SDN кожним модулем, таким як шасі, маршрутизатори та вузли в мережі. Крім того, SDN вважається життєздатним рішенням, де для виконання завдання можна використовувати мінімальні ресурси без погіршення загальної продуктивності мережі (наприклад, безпеки), що зменшує споживання енергії.

Наприклад, можна розглянути модель вимірювання, де для експерименту розглядається потужність, споживана комутаторами OpenFlow, такими як апаратний комутатор OF та vSwitch, що працюють на сервері. Згідно з отриманими результатами, увімкнення механізмів «сну» може покращити енергоефективність OF vSwitch, оскільки енергоспоживання мережі залежить від кількості активних з'єднань у мережі. Додаткової економії до 6,6% загальної потужності можна досягти, встановивши швидкість конфігурації порту 10 Мбіт/с. Очікується, що отримані вимірювання потужності матимуть похибку менше 1% в апаратних комутаторах і 8% у програмному забезпеченні. Часте вимикання та ввімкнення живлення може продемонструвати свій вплив на зменшення терміну служби мережевих робочих пристроїв. Ефективність може бути досягнута лише тоді, коли прийняті схеми не впливають на продуктивність системи. Отже, метод, який буде реалізовано в мережі, слід вибирати на основі характеристик мережі.

Враховуючи отримані результати, можна розглянути енергоефективні схеми, які можливо і доцільно реалізувати в SDN.

Енергоефективність через оптимальне використання мережевих ресурсів. Обсяг трафіку в різний час доби неоднаковий, особливо в нічний час навантаження трафіку може значно зменшитися і більшість вузлів у мережі залишаються невикористаними або недостатньо використаними (як показано на рисунку 10). Однак, коли реалізуються методи захисту безпеки, енергоспоживання значно зростає. У SDN, завдяки гнучкості керування мережевими пристроями за допомогою мови програмування високого рівня, методи переадресації можуть бути реалізовані з легкістю. Контролер у SDN може приймати рішення відповідно до навантаження трафіку у системі, сприяючи екологічним мережам та ефективному використанню ресурсів. Вузли, які не мають трафіку, можуть бути відправлені в сплячий режим, а для вузлів з низьким трафіком, трафік може бути перенаправленим до кількох активних мереж для надання послуги. Це призводить до енергоефективного належного використання мереж.

Метод на основі контенту був реалізований у програмно визначеній інформаційно-центричній мережі (Information Centric Network - ICN) для належного використання ресурсів зі зниженим енергоспоживанням у мережі. ICN має попередню інформацію про обсяг контенту, який потрібно доставити і виділяє лише необхідну кількість ресурсів. Цей метод також відстежує ці ресурси для забезпечення належного використання. Модель еластичного дерева, показала 50% зниження енергоспоживання, де модуль оптимізатора виділяє найбільш підходящий зв'язок для ефективної обробки навантаження трафіку при дотриманні вимог QoS. Невикористані з'єднання в мережі переходять у сплячий режим для економії енергії.

Multi Layer Traffic Engineering (MLTE) і GreCO дотримуються подібного підходу, як еластичне дерево і ці підходи незначно економлять енергоспоживання в SDN. Алгоритм ексклюзивної маршрутизації (EXR) маршрутизує трафік на основі вимірювання часу і цей метод маршрутизації більш ефективний і швидкий порівняно з іншими алгоритмами енергозбереження. Також пропонуються протоколи енергоефективної маршрутизації для маршрутизації мережевого трафіку до найбільш прийнятного та найкоротшого шляху для задоволення вимог користувачів. Процес проектування черги був прийнятий для енергозбереження комутатора OpenFlow на платформі NETFPGA. Контролер годинника поєднується з контролером OpenFlow для підтримки різних режимів керування живленням. Цей метод має окремий модуль, який знижує частоту до 0 МГц в умовах відсутності трафіку для належного використання потужності. Зменшення реплікації небажаних даних може певною мірою зменшити енергоспоживання мережі. Щоб уникнути надмірності в зберіганні даних, був реалізований метод SMart In-Network Duplication (SMIND). Цей метод ідентифікує надлишкові дані за допомогою техніки відбитків пальців.

Енергоефективне проектування/управління трафіком. Проектування/управління трафіком для оптимізації енергії не є новою концепцією. Цей підхід популярний у традиційних мережах і використовується в SDN для енергоефективності. Мережа асинхронного режиму передачі (Asynchronous Transfer Mode - ATM) має суворі та обмежені політики для захисту

всієї мережі без погіршення якості обслуговування (QoS) користувачів. Ці функції є корисними для SDN. Методи управління потоком і балансування навантаження можуть бути реалізовані як в комутаторах, так і в контролері для енергоефективності в SDN. Споживання енергії зведено до мінімуму в традиційних мережах на основі Інтернет-протоколу (IP) за допомогою балансування навантаження та ефективних шляхів маршрутизації, таких як протоколи маршрутизації за найкоротшим шляхом. Ці функції також розглядаються як схеми енергозбереження в SDN. Подібним чином, протокол комутації Multi Protocol Label Switching (MPLS) здебільшого зосереджений на реалізації схем проектування трафіку (TE) в інфраструктурі Інтернету для ефективної доставки пакетів з оптимальною енергією. Цей метод підходить для проектування трафіку в SDN, де недоліки MPLS можуть бути усунені за допомогою мереж OpenFlow.

ECMP (Equal-Cost Multi-Path) на основі хешування було запропоновано як схему балансування навантаження на основі комутатора рівної вартості, яка спрямовує потік на кілька шляхів у мережі для підвищення енергоефективності. Основними недоліками цього методу балансування навантаження є обчислювальна складність і низька продуктивність. Hedera (загальнодоступна мережа з відкритим кодом, якою керують провідні організації з усього світу) розглядається як інтелектуальна схема балансування навантаження, здатна обробляти великі потоки. У Hedera контролер керує трафіком на основі інформації, отриманої від комутаторів і споживає мінімум енергії.

Це допомагає уникнути зіткнень. Mahout, схема балансування навантаження, була реалізована в центрах обробки даних для підвищення продуктивності мережі та зменшення споживання енергії. Балансування навантаження DevoFlow було реалізовано у корпоративних мережах і середовищах центрів обробки даних, щоб зменшити навантаження на контролер, надаючи комутаторам набір додаткових правил підстановки та мінімізуючи загальне споживання енергії. Інші переваги цього методу включають продуктивність і масштабованість. Підхід під назвою DIFANE був здатний досягти балансування навантаження контролера шляхом впровадження детальних і суворих політик у корпоративних мережах. Мета DIFANE подібна до DevoFlow, однак ця схема додає додаткові комутатори в мережу, які називаються комутаторами повноважень, які зберігають усі важливі записи потоку. Якщо пакет не відповідає правилам таблиці потоків у звичайних комутаторах, вони негайно пересилаються комутаторам повноважень для прийняття рішення. Hyperflow було запропоновано як платформу розподіленої площини керування на основі подій, яка може забезпечити переваги OpenFlow, а також подолати його обмеження масштабованості. Balance Flow було запропоновано як схему балансування навантаження контролера в мережах OpenFlow. Його було запропоновано як розширення в комутаторах OpenFlow під назвою Controller X action. Це класифікує потоки за різними категоріями на основі комутаторів, з яких вони походять і спрямовує їх до іншого контролера. Розробка трафіку SDN/OSPF (SOTE) була запропонована як гібридний метод проектування трафіку з комбінацією спочатку відкритого найкоротшого шляху та SDN для зниження використання каналу зв'язку в мережі. Основою метою цього методу є балансування навантаження шляхом рівномірного спрямування їх через усі вузли SDN та мінімізації загального споживання енергії.

Енергоефективне оновлення політики SDN, включаючи політики безпеки. Звичайні мережі час від часу оновлюють мережеві політики, тоді як SDN, будучи адаптивною архітектурою, потребує частого оновлення, щоб адаптуватися до оновленого середовища. Постійні оновлення в системі можуть перешкоджати продуктивності мережі, а також збільшувати енергоспоживання. У SDN контролер відповідає за оновлення та впровадження нових політик у мережі. Щоразу, коли нова політика оновлюється в мережі, усі комутатори в мережі отримують і зберігають її разом із номером версії. Якщо в комутаторах існує кілька політик, пакет розрізняється на основі номера версії та обробляється за допомогою нової політики або старої політики.

Розглянемо метод з оновленням узгодженості кожного пакета та узгодженості всіх пакетів у SDN. Контролер SDN своєчасно оновлює систему та усуває старі політики, коли він перестає

отримувати пакети за допомогою старих версій. Деякі інші контролери встановлюють дату закінчення терміну дії для старіших версій і не підтримують їх після цієї фіксованої дати. Основне обмеження цього методу полягає в тому, що він повинен зберігати обидві версії в таблиці потоку протягом певного часу. Це може перевантажити записи таблиці потоків, зайняти більше місця в пам'яті та збільшити споживання енергії. Новий метод, який має справу з єдиним набором правил, може спряти вирішенню проблем споживання пам'яті та споживання енергії. У методі TIMECONF нові політики оновлюються послідовно в запланований час. Однак цей метод пов'язаний із деякою затримкою, оскільки контролер оновлює наступний комутатор лише після отримання підтвердження від оновленого комутатора. Метод поступового оновлення під назвою Net-Plumber для забезпечення швидкого оновлення політики в мережі шляхом налаштування лише тієї частини комутаторів, яка потребує оновлення, що призводить до зниження споживання енергії. Він розташований між площиною даних і площиною керування та впроваджує політики в комутатори зі швидкістю 50–500 мкс. Зауважимо, що енергію можна заощадити в SDN, знизивши швидкість з'єднання під час оновлення політик SDN. Зауважимо, що політику SDN можна легко оновити за допомогою з'єднань зі швидкістю 10 Мбіт/с у режимі реального часу та споживати на 4 Вт менше, ніж з'єднання зі швидкістю 1 Гбіт/с.

Енергоефективний моніторинг умов трафіку. Енергозбереження в мережі можна отримати шляхом динамічного програмування мережі відповідно до умов трафіку. Щоб динамічно налаштовувати систему на основі потоку трафіку, необхідно мати оновлену інформацію про стан трафіку в мережі. Це вимагає впровадження підходів до моніторингу трафіку в SDN. Хоча ці схеми моніторингу не зовсім точні, вони можуть допомогти контролеру мати уявлення про потік трафіку в мережі, включаючи атаки на безпеку мережі.

Підхід під назвою Open TM був запропонований як система моніторингу на основі запитів, яка покладається на функції комутаторів OpenFlow для вимірювання мережевого трафіку. Інформацію не можна отримати з усіх комутаторів, оскільки це може призвести до навантаження на мережу та споживання енергії. Комутатор, з якого збирається статистика трафіку, вибирається з урахуванням інформації про маршрутизацію, наявної в контролері, щоб мінімізувати споживання енергії та підвищити загальну продуктивність мережі. Payless було представлено як схему моніторингу трафіку на основі залучення, яка використовує адаптивний алгоритм збору статистики для отримання умов трафіку з високою безпомилковістю у всій мережі. У цьому методі контролер постійно запитує комутатори в площині даних щодо оновлень щодо потоку трафіку. Payless виявилася ефективним методом, знизивши енергоспоживання в мережі. Недоліком цієї системи є постійне запитування контролера для підтримки точності, що може спричинити накладні витрати на контролер.

FlowSense було запропоновано як метод моніторингу на основі push, який фокусується на оцінці використання каналу. Комутатори пересилають повідомлення про виявлення нових потоків до контролера за допомогою команд PacketIn і FlowRemoved, на основі яких контролер вводить нові політики в систему. Ці повідомлення можуть сприяти схемі моніторингу FlowSense для оцінки використання ресурсів, ширини смуги та споживання енергії в мережі. OpenSketch було запропоновано як схему моніторингу потоку трафіку на основі push, яка дотримується подібної концепції роз'єднання площин, як SDN і використовує три основні етапи, а саме хешування, фільтрацію та підрахунок. Хешування використовується для надання короткого огляду потоків, які необхідно виміряти. Етап фільтрації усуває непотрібні дані, а статистика отримується на етапі підрахунку. Отримані результати мають високу точність. MicroTE було запропоновано як схему моніторингу трафіку в мережі. Він динамічно адаптується до умов трафіку в мережі та негайно реагує на зміни в мережі. Оновлення щодо останніх умов трафіку, отримані від агента, встановленого на сервері, негайно повідомляються контролеру. OpenSample було запропоновано як схему моніторингу на основі push, яка покладається на інструмент вибірки пакетів sFlow для отримання заголовків пакетів із мережі.

Ternary Content Addressable Memory (TCAM) Compression для енергоефективності та безпеки мережі. Правила, які мають бути реалізовані в SDN, зберігаються в таблиці

потоків, наявній у адресній пам'яті TCAM. Він може порівнювати всі вхідні потоки паралельно та забезпечувати швидку обробку пакетів. Кількість записів у таблиці потоку обмежена, оскільки використання TCAM пов'язане з фактором вартості. Очікується, що TCAM накладе тягар у 400 разів більше вартості та у 100 разів більше споживання електроенергії, ніж традиційні пристрої зберігання пам'яті, такі як RAM. Іншою основною проблемою TCAM є її час оновлення, обмежений 40–50 таблицями правил на секунду.

Був запропонований компактний TCAM, який згущує структуру TCAM шляхом зменшення розміру ідентифікаторів потоків у таблиці потоків. Потокам призначено певний ідентифікатор потоку з метою ідентифікації. Ще однією перевагою компактного TCAM є використання SDN для видалення зайвої інформації. За допомогою компактного методу TCAM можна досягти 80% зниження потужності. Бритва TCAM була запропонована для зменшення кількості записів потоку в таблиці потоків шляхом реалізації чотириступінчастого механізму, який стискає TCAM на 29,0%, що призводить до економії 54% енергії. У цьому методі багатовимірні правила фрагментовані на багато одновимірних списків правил. BitWeaving було запропоновано як безпрефіксний потрійний класифікатор, реалізований для стиснення правил у TCAM з використанням двох різних підходів: заміна бітів і злиття бітів. У цьому методі записи потоку з однаковим рішенням, які відрізняються лише одним бітом, можуть бути об'єднані разом. Метод BitWeaving зміг досягти ступеня стиснення 23,6% з високою швидкістю та енергоефективністю.

Розподіл палітри був запропонований для вирішення проблеми розміщення правил шляхом розбиття великих таблиць SDN на невеликі підтаблиці за допомогою декомпозиції опорних бітів. Оскільки всі правила не можуть зберігатися в одній мережі, вони розділені та розподілені між кількома мережами під SDN. Був запропонований метод спільної оптимізації, який використовує як розподіл правил, так і інженерію трафіку для досягнення оптимізації енергії та безпеки в мережі.

Правильне розміщення пристроїв SDN для енергоефективності та безпеки мережі. Оскільки контролер SDN розглядається як мозок SDN для керування поведінкою мережі, його розташування відіграє вирішальну роль. Контролер повинен мати можливість керувати наданою кількістю комутаторів у мережі. Правильне розміщення контролера може підвищити загальну ефективність SDN, а також може сприяти зниженню витрат. Розгортання багатьох контролерів у SDN має як плюси, так і мінуси. Було проведено значну кількість досліджень контролерів SDN, які необхідно інтегрувати в систему. Кількість контролерів у SDN має ґрунтуватися на кількості навантаження трафіку та вимогах до безпеки мережі, а також розмірі мережі, яку контролер повинен контролювати. Була запропонована математична модель для розміщення контролерів з мотив для мінімізації витрат на енергію та підвищення продуктивності мережі. Враховуються такі фактори, як розташування комутаторів, довжина та пропускна здатність комутаторів та інша інформація. Проблема розміщення контролера для мінімізації витрат може бути виражена у вигляді:

$$C_c(x) + C_l(v) + C_t(z), \tag{1}$$

де $C_c(x), C_l(v), C_t(z)$ – вартість встановлення комутаторів, вартість підключення контролерів до комутаторів та вартість зв'язування контролерів між собою відповідно.

Рівняння (1) має задовольняти певним критеріям, таким як кількість комутаторів, підключених до мережі, завжди менша за кількість портів у мережі, комутатори в мережі мають лише одне конкретне посилання для підключення до мережі, контролер здатний обробляти кількість пакетів, надісланих комутаторами, підключеними до певного контролера.

Крім того, розміщення віртуальної машини в SDN забезпечує належне використання ресурсів інфраструктурою в мережі. Хоча віртуальні машини використовуються в мережі для покращення енергозбереження. Неправильне та надмірне розміщення віртуальних машин може погіршити загальну продуктивність і безпеку мережі, а також збільшити споживання енергії.

Висновки

Вибір різних параметрів SDN залежить від додатків, які передбачається підтримувати SDN. Наприклад, оптимальні параметри SDN можуть не бути оптимальними параметрами SDN для традиційних мереж центрів обробки даних, а оптимальні SDN для IoT можуть не бути оптимальними SDN для кіберфізичних систем тощо. Робота повинна бути зосереджена на розробці механізмів безпеки з низьким енергоспоживанням, які можуть підвищити загальну продуктивність мережі з високою видимістю та масштабованістю.

Список використаної літератури:

1. SDN: Software Defined Networks: An Authoritative Review of Network Programmability Technologies, Thomas D. Nadeau, Ken Gray. Copyright © 2013. All rights reserved. Printed in the United States of America. Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472. – p. 382

2. Абдельхамід Меллук, Фетія Баннур, Самі Суїхі. Software-Defined Networking 2: Extending SDN Control to Large-Scale Networks. Wiley. John Wiley & Sons, LTD, 2023 – p. 176.

3. Гніденко М.П., Вишнівський В.В., Ільїн О.О. Побудова SDN мереж. – Навчальний посібник. – Київ: ДУТ, 2019. – 190 с.

4. Beakal Gizachew Assefa, Öznur Özkasap. A Survey of Energy Efficiency in SDN: Software-based Methods and optimization models. Journal of Network and Computer Applications. Volume 137, 1 July 2019, Pages 127-143

5. Гніденко М.П., Прокопов С.В., Гніденко М.М. Підвищення безпеки програмно-визначених мереж (SDNs). / Київ: ДУТ. Наукові записки ДУТ – 2023. – №2(4). – с. 54-65.

Автори статті

Гніденко Микола – кандидат технічних наук, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0009-0002-5261-3581

Гніденко Максим – аспірант, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0009-0008-4450-6472

Вишнівський Олександр – аспірант, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0009-0008-0209-9549

Зінченко В'ячеслав – аспірант, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0009-0000-7087-1678

Authors of the article

Hnidenko Mykola – Candidate of Science (technic), Associate Professor, State University of Information and Communication Technology, Kyiv, Ukraine.

ORCID: 0009-0002-5261-3581

Hnidenko Maksym – postgraduate, State University of Information and Communication Technology, Kyiv, Ukraine.

ORCID: 0009-0008-4450-6472

Vyshnivskyi Oleksandr – postgraduate, State University of Information and Communication Technology, Kyiv, Ukraine.

ORCID: 0009-0008-0209-9549

Zinchenko Vyacheslav – postgraduate, State University of Information and Communication Technology, Kyiv, Ukraine.

ORCID: 0009-0000-7087-1678