УДК 004.056:004.75:004.89
DOI https://doi.org/10.32782/2663-5941/2026.3.1/10

Єрошенко О.А.
https://orcid.org/0000-0001-6221-7158
Харківський національний університет радіоелектроніки

Федорченко В.М.
https://orcid.org/0000-0001-7359-1460
Харківський національний університет радіоелектроніки,
Харківський національний економічний університет імені Семена Кузнеця

Партика С.О.
https://orcid.org/0000-0002-7376-8980
Харківський національний університет радіоелектроніки

Пивоварова Д.І.
https://orcid.org/0000-0002-7251-994X
Харківський національний університет радіоелектроніки

МЕТОД ВИЯВЛЕННЯ DDOS-АТАК НА КОНТРОЛЕР SDN НА ОСНОВІ ІНФОРМАЦІЙНОЇ ЕНТРОПІЇ ВИЩОГО ПОРЯДКУ

Статтю присвячено вирішенню актуальної проблеми забезпечення безпеки програмно-конфігурованих мереж (SDN), зокрема захисту рівня управління мережи від розподілених атак на відмову в обслуговуванні (DDoS). Унікальна архітектура SDN, що відокремлює площину управління від площини даних, робить централізований контролер критичною точкою відмови та головною мішенню для зловмисників, оскільки перевантаження ресурсу Packet-In призводить до повної деградації мережі.

У роботі проаналізовано недоліки існуючих методів статистичного аналізу, які зазвичай фокусуються лише на множені IP-адрес без урахування динамічних часових факторів, що робить їх вразливими до складних стратегій атак, таких як інтелектуальний спуфінг. Авторами запропоновано вдосконалений метод виявлення DDoS-атак, що базується на використанні інформаційної ентропії вищого порядку та статистичної моделі розподілу Пуассона. Суть методу полягає в прецизійному аналізі швидкості потоку пакетів у межах фіксованих часових вікон. Моделювання процесу надходження запитів як пуассонівського процесу дозволяє точніше ідентифікувати аномальні коливання трафіку: за нормальних умов ентропія залишається стабільно високою через статистичну випадковість потоків, тоді як під час атаки вона стрімко падає внаслідок штучної концентрації трафіку на конкретних вузлах.

Експериментальна перевірка методу проводилася з використанням розгалуженої топології в емуляторі Mininet, комутатора Open vSwitch та контролера Ryu. Результати моделювання підтвердили, що запропонований підхід забезпечує вищу точність детектування та суттєво менший рівень обчислювальних помилок для різних стратегій атак порівняно з традиційними рішеннями. Встановлено, що оптимальним для стабільного виявлення аномалій є часове вікно тривалістю 10 секунд. Додатково впроваджена система «кредитів довіри» для IP-адрес дозволяє ефективно фільтрувати шкідливий трафік на рівні граничних комутаторів, зберігаючи дефіцитні ресурси контролера для обслуговування легітимних запитів, що гарантує високу доступність та стійкість мережевої інфраструктури навіть в умовах інтенсивного кібервпливу.

Ключові слова: *програмно-конфігуровані мережі, контролер SDN, DDoS-атаки, інформаційна ентропія, розподіл Пуассона, кібербезпека, часове вікно, експоненційне згладжування.*

Постановка проблеми. У сучасному цифровому середовищі мережеві загрози набувають дедалі більшого поширення. Розподілені атаки на відмову в обслуговуванні (DDoS), продовжують створювати серйозні виклики. Для забезпечення сталої роботи різноманітних сервісів вкрай важливо посилити мережевий захист та підвищити загальний рівень безпеки. Серед численних передових заходів безпеки яскраво виділяється стратегія захисту на основі програмно-конфігурованих мереж (SDN), яка стала зразком для впровадження інтелектуального та гнучкого управління безпекою.

Унікальна архітектура SDN відокремлює площину управління від площини даних. Цей підхід наділяє управління та контроль мережевим трафіком гнучкістю й точністю, які раніше були недосяжними. Зіткнувшись із DDoS-атакою, SDN може повною мірою продемонструвати свої можливості. Спираючись на функцію моніторингу в режимі реального часу, вона здатна швидко виявляти аномальні стани трафіку та оперативно налаштовувати механізми реагування. За допомогою SDN персонал з експлуатації та обслуговування систем безпеки може динамічно планувати маршрути трафіку, вміло уникати перевантажених та атакованих ділянок мережі, а також швидко ізолювати шкідливий трафік. Водночас це дозволяє оптимізувати розподіл мережевих ресурсів для гарантованого проходження критично важливого бізнес-трафіку, ефективно протистоячи бурхливим потокам даних (флуду), спричиненим DDoS-атаками [1]. Стратегія підкреслює гнучкість та інноваційність архітектури мережевого захисту й процесів управління безпекою, надаючи персоналу розширені можливості контролю та негайного втручання. Усе це комплексно підвищує стійкість мережевої інфраструктури та мінімізує негативні наслідки від DDoS-атак.

Аналіз останніх досліджень і публікацій. Розподілені додатки стають дедалі складнішими, а традиційні мережі – громіздкими. Інтегрована передача даних і управління перешкоджають досягненню високої гнучкості та ефективного розподілу ресурсів в управлінні мережею, створюючи серйозну перешкоду для прогресу.

Наявність прикладного рівня та зв'язок між рівнем управління і рівнем даних значно підвищили програмованість, масштабованість та відкритість мережі завдяки API та «північним» інтерфейсам, що полегшує управління мережею та налаштування додатків [1].

В архітектурі SDN [2] контролер SDN є головною мішенню зловмисників для отримання управління мережевими ресурсами. DDOS-атака, спрямована на контролер, швидко перевантажує мережу, порушуючи її нормальну роботу та виснажуючи критично важливі ресурси, такі як кеш-пам'ять і пропускна здатність мережевих пристроїв та контролерів. Хоча програмно-конфігуровані мережі (SDN) мають такі механізми протидії DDOS-атакам, як моніторинг, програмоване користувацьке виявлення, візуалізація мережі та контроль деталізації (гранулярності), вони все ще перебувають на стадії становлення, стикаючись із проблемами інтеграції, методами вирішення завдань та питаннями стабільності контролерів [3].

Постановка завдання. Метою статті є створення безпечнішого, ефективнішого та надійнішого мережевого середовища для різноманітних додатків, що має вирішальне значення для подальшого розвитку мережевих технологій.

Виклад основного матеріалу. Архітектурне відокремлення рівня управління від рівня даних у програмно-конфігурованих мережах робить безпеку рівня управління пріоритетною. Модель централізованого управління підкреслює необхідність надійного захисту від DDoS-атак, зокрема тих, що спрямовані на контролери SDN. Виявлення таких атак та захист від них є критично важливими для підтримання стабільної роботи мережі. Визначення пріоритетності безпеки рівня управління є необхідною умовою для забезпечення загальної безпеки та надійності мережі [4].

У сфері програмно-конфігурованих мереж проблема виявлення розподілених атак на відмову в обслуговуванні привертає значну увагу. Існуючі контролери SDN, такі як Nakashima, використовують методи статистичного аналізу для ідентифікації подібних атак. Однак ці методи зосереджені переважно на концентрації IP-адрес джерела та призначення без урахування часових аспектів, що призводить до неповної інтеграції функцій SDN та вразливості до атак. У випадку DDoS-атак на контролери SDN зловмисники часто переповнюють контролер пакетами, що призводить до виснаження його ресурсів. Аналізуючи ентропію IP-інформації, ці методи мають на меті виявити аномалії в патернах трафіку [5]. Для розширення можливостей виявлення вкрай важливо розробити складніші методи, які враховуватимуть не лише статистичні характеристики, але й часові фактори та специфічні способи спрямування атак на контролери SDN. Поєднуючи ці підходи, дослідники зможуть краще підготувати контролери SDN до протидії DDoS-атакам і забезпечити безпеку та стійкість мережі перед обличчям новітніх кіберзагроз [4].

Для вирішення цієї проблеми запропоновано метод виявлення DDoS-атак на контролери SDN з використанням вищої інформаційної ентропії. Цей підхід зосереджений на ідентифікації унікальних характеристик DDoS-атак на контролери SDN шляхом впровадження системи виявлення швидкості потоку пакетів. Він передбачає передачу даних комутатора до контролера в межах заданого часового вікна, що дозволяє більш ефективно та результативно виявляти DDoS-атаки.

Таким чином, значення ентропії для кожної точки в часовому вікні можуть обчислюватися в режимі реального часу і порівнюватися з обраним пороговим значенням після формування вибірки та аномальної вибірки, щоб визначити, чи зазнає контролер SDN DDoS-атаки. Метод виявлення поєднує патерни зв'язку між комутатором і контролером з аналізом швидкості потоку DDoS-атаки для ефективного і точного виявлення та пом'якшення потенційних загроз [6]. Ентропія трафіку в часовому вікні обчислюється за формулою інформаційної ентропії з урахуванням стану розподілу пакетів, представленого перетворенням у часі під час передачі до контролера [7].

Якщо зловмисник розпочинає DDoS-атаку на контролер SDN, раптово відбувається різке збільшення трафіку в заданому часовому вікні незалежно від стратегії формування пакета який атакується, що призводить до зниження інформаційної ентропії. Завдяки цьому унікальному механізму, даний метод ефективно інтегрує функції SDN, точно виявляє DDoS-атаку на контролер, успішно нівелює негативний вплив стратегії зловмисника на показник виявлення, значно підвищує точність і надійність детектування, а також забезпечує високий рівень безпеки контролера SDN.

Метод статистики інформаційної ентропії на основі розподілу Пуассона відіграє важливу роль у методі виявлення DDoS-атак на контролери SDN. Розподіл Пуассона – це статистичний інструмент, який допомагає прогнозувати частоту випадкових подій, таких як надходження пакетів, у межах певного часу та простору. Ця модель може бути особливо корисною у сценаріях, коли контролеру SDN необхідно виявити розподілену атаку на відмову в обслуговуванні шляхом аналізу вхідних пакетів даних [8]. Моделюючи процес надходження пакетів як пуассонівський процес, можна більш точно проаналізувати патерни розподілу трафіку. Це забезпечує наукове та об'єктивне підґрунтя для статистики інформаційної ентропії. Обчислюючи інформаційну ентропію на основі розподілу Пуассона, можна точніше фіксувати зміни аномальної швидкості потоку, покращити здатність виявлення DDoS-атак, ефективно відрізняти нормальні коливання швидкості потоку від аномалій, спричинених атакуючим трафіком, зробити результати перевірки більш точними та надійними, заощадити дорогоцінний час для своєчасного вжиття захисних заходів, а також гарантувати надійну безпеку та стабільність рівня управління мережею SDN.

Концепція інформаційної ентропії здебільшого використовується для опису невизначеності випадкових величин [3]:

$$H = -\sum_{i=1}^{n} p_i \log p_i, \qquad (1)$$

де H – інформаційна ентропія, p_i – ймовірність появи і-ї події, n – кількість можливих результатів (значень) випадкової величини.

У мережевому середовищі SDN за умов нормального трафіку швидкість мережевого потоку є більш випадковою, тому інформаційна ентропія стає більшою. Коли ж швидкість потоку під час DDoS-атаки стає аномально високою, розподіл швидкості мережевого потоку одразу стає передбачуваним, трафік сильно концентрується, і інформаційна ентропія значно зменшується. Базуючись на цій властивості, багато дослідників застосовують інформаційну ентропію для виявлення мережевих аномалій.

Наразі існують два основні статистичні методи для виявлення DDoS-атак на контролер SDN. Перший метод аналізує ентропію інформації про цільову IP-адресу в пакеті, надісланому від комутатора SDN до контролера, тоді як другий метод зосереджується на ентропії інформації про IP-адресу джерела в пакеті даних, переданому від комутатора SDN до контролера. Ці методи ґрунтуються на розумінні розподілу підробки IP-адрес джерела під час DDoS-атак та концентрованої природи інформації про цільові IP-адреси. Використовуючи дані про передачу пакетів у режимі реального часу, можна обчислити ймовірність збігу як для IP-адреси джерела, так і для цільової, що дозволяє визначити значення ентропії інформації про IP-адресу джерела або цілі шляхом застосування формули інформаційної ентропії. Цей підхід дозволяє ідентифікувати потенційні DDoS-атаки шляхом аналізу патернів розсіювання (дисперсії) IP-інформації.

У сфері DDoS-атак, спрямованих на контролери SDN, зловмисники використовують такі складні методи, як підробка IP-адреси джерела (спуфінг) та імітація бажаних IP-адрес [5]. Ці так-

тики маніпулюють правилами таблиць потоків на комутаторах, зрештою спрямовуючи пакети до контролера, що призводить до збою системи. Це створює серйозну проблему для традиційних методів статистичної ентропії щодо розрізнення різноманітних стратегій атак. Як наслідок, існуючим механізмам захисту може бути важко ефективно боротися з цими еволюціонуючими загрозами. Для експертів з безпеки вкрай важливо розробити більш надійні та адаптивні стратегії для захисту інфраструктур SDN від подібних зловмисних дій.

Запропонований статистичний метод використовує інформаційний розподіл Пуассона для аналізу розподілу потоку інформаційної ентропії, пропонуючи свіжий погляд на аналіз даних. Мета цього методу полягає в отриманні інформації про розподіл швидкості потоку для обчислення ентропії пакетів на основі даних, наданих комутатором. Навіть якщо зловмисник ініціює DDoS-атаку на контролер, використовуючи будь-яку стратегію атаки, раптовий трафік DDoS-атаки неминуче змінить розподіл трафіку пакетів, що передаються до контролера.

Припускаючи, що ймовірність того, що контролер отримує пакет за одиницю часу від комутатора, є величиною λ, вираз (2) можна використати для доведення того, що процес надсилання пакета переривання до контролера підпорядковується розподілу Пуассона.

Повідомлення із запитом на комутацію до контролера для переходу до періоду T розглядається в дослідженні як незалежна випадкова величина. Цей елемент відіграє вирішальну роль у безперервному процесі оптимізації та управління. Це означає, що немає жодного зв'язку між повідомленнями із запитами, отриманими протягом різних періодів, і кожне повідомлення із запитом є випадковим та не впливає на інші періоди.

Розділивши період часу t на n менших періодів, k пакетів, отриманих протягом періоду t, можна вважати рівномірно розподіленими між цими n періодами. Ймовірність того, що період t міститиме k пакетів протягом n періодів. Цей метод дозволяє точно визначити розподіл ймовірностей надходження пакетів у межах заданого часового проміжку.

$$p_k(t) = C_k^n(\lambda\Delta t)^k(1-\lambda\Delta t)^{n-k} \qquad (2)$$

Розподіл Пуассона використовується для моделювання надходження пакетів від комутатора до контролера за умови виконання специфічних умов [7]. Коли ці умови виконуються, вхідні запити в момент часу *t* підпорядковуються розподілу Пуассона, що дозволяє описати профіль трафіку з точки зору кількості запитів, отриманих контролером від комутатора. Профіль Пуассона ефективно відображає потік вхідного пакетного трафіку в цій комунікаційній системі.

Для ефективного аналізу пакетного трафіку ретельно підбираються кількість та тривалість статистичних часових вікон для відстеження пакетів, що надсилаються від комутатора до контролера, що дозволяє отримувати точні статистичні дані щодо вхідного пакетного трафіку. Завдяки оптимізації цих параметрів можна ретельно відстежувати продуктивність мережі та управляти нею. Результати статистики в режимі реального часу обробляються за допомогою формули розподілу Пуассона. На основі результатів обробки будується розподіл швидкості потоку для кожного часового вікна, а значення ентропії цього розподілу обчислюється за допомогою формули інформаційної ентропії.

Для боротьби з DDoS-атаками на контролери SDN запроваджено новий метод до виявлення з використанням розширеної інформаційної ентропії. Як рішення було розроблено модель виявлення, зображену на рисунку 1. Метод має на меті ефективне реагування на загрози безпеці та підтримання стабільності мережі. Модель ретельно розроблена з урахуванням характеристик мережі SDN та моделі поведінки під час DDoS-атаки. Принцип інформаційної ентропії ефективно використовується для аналізу розподілу швидкостей потоку всередині контролера під час процесу перетворення.

За умов нормального потоку швидкість мережевого трафіку розподіляється відносно випадково, тоді як DDoS-атака спричиняє швидку та раптову концентрацію розподілу трафіку, внаслідок чого інформаційна ентропія стрімко падає. Спираючись на цю суттєву відмінність, модель виявлення здатна точно фіксувати аномальні зміни потоку, а контролер SDN може ефективно виявляти DDoS-атаки. Порівняно з традиційними методами виявлення, ця модель не обмежується статистикою даних IP-адрес джерела та призначення пакетів, а ефективно враховує розподіл усього трафіку. Вона успішно усуває недоліки традиційних методів під час протидії різним стратегіям атак, значно підвищує точність і надійність виявлення DDoS-атак у контролері SDN, а також забезпечує потужну технічну підтримку для гарантування безпеки та стабільності цілей управління мережею SDN.

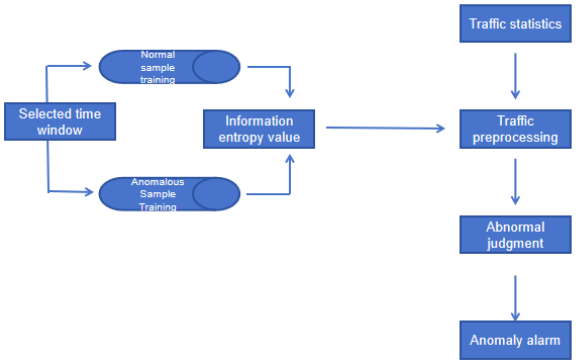

Рис. 1. Схема моделі виявлення DDoS-атак на контролер SDN

Для моделі виявлення, зображеної на рисунку 1, першим кроком є науково обґрунтоване та раціональне визначення відповідних параметрів часового вікна, зокрема його розміру та тривалості. Точний вибір цих двох параметрів відіграє важливу роль у загальній ефективності виявлення.

Створюються два набори вибірок трафіку – один із нормальною швидкістю потоку, а інший з аномальною, із заздалегідь визначеними критеріями розміру та тривалості. Після навчання на цих вибірках необхідний інструмент статистичного аналізу для визначення порогу верифікації інформації для методу виявлення. Поріг обчислюється на основі результатів процесу навчання, що дозволяє точно ідентифікувати аномальні патерни трафіку. Дане порогове значення використовується як правило прийняття рішень, за яким швидкість потоку в реальному часі класифікується як нормальна або аномальна.

В очікуванні встановлення порогового значення контролер ретельно проводить статистичний аналіз у режимі реального часу, точно відстежуючи кількість груп (пакетів) у межах кожного часового вікна. З використанням моделі розподілу Пуассона обчислюються ймовірності появи різної кількості груп у межах кожного часового вікна, після чого визначається значення ентропії, пов'язане з даними трафіку в цей проміжок часу. Такий ретельний обчислювальний підхід дає цінне розуміння патернів трафіку, представляючи їх у вигляді інформаційної ентропії. Завдяки цьому контролер отримує критично важливі дані для прийняття обґрунтованих рішень щодо стратегій управління трафіком. Отримавши значення ентропії для часового вікна, воно точно порівнюється із заздалегідь визначеним пороговим значенням. Порівняльний аналіз дозволяє чітко встановити, чи є поточний трафік аномальним чи нормальним, і ефективно виявити, чи зазнає контролер SDN DDoS-атаки.

Для точного аналізу регулярних патернів трафіку надзвичайно важливо ретельно вибрати розмір вікна *n* та тривалість *t* для кожного часового вікна. Шляхом статистичного аналізу нормального трафіку в цих обраних часових вікнах можна сформувати репрезентативну вибірку. Метод дозволяє отримати всебічне розуміння типової поведінки трафіку.

Підготовка трафіку передбачає управління швидкостями потоків в реальному часі за допомогою статистики ентропії та розподілу Пуассона. Метод допомагає підтримувати стабільний потік трафіку шляхом аналізу даних і відповідного коригування для забезпечення ефективної роботи систем передачі даних. Ймовірність потоку в кожному часовому вікні обчислюється на основі рівняння розподілу Пуассона. Значення інформаційної ентропії для N часових вікон обчислюється на основі формули інформаційної ентропії. Використовуючи кілька стандартних вибірок потоку, результати навчання обчислюються та вимірюються, а метод статистичного аналізу застосовується для обчислення середньої ентропії, дисперсії, довірчого інтервалу, максимального довірчого інтервалу та мінімального довірчого інтервалу результатів для кількох стандартних вибірок трафіку.

Навчальний модуль для моделі аномального потоку передбачає попередню обробку швидкостей аномальних потоків у реальному часі з використанням фіксованого розміру часового вікна n та тривалості вікна t. Препроцесор потоку спеціально націлений на аномальні швидкості потоку, що обчислюються в режимі реального часу за допомогою методу статистики інформаційної ентропії на основі розподілу Пуассона. За допомогою рівняння розподілу Пуассона визначається ймовірність потрапляння аномальних потоків у кожне часове вікно, що веде до обчислення значення інформаційної ентропії в межах часового вікна. Процес дозволяє виявляти та аналізувати аномальні швидкості потоку для підвищення точності та ефективності систем виявлення аномалій. По суті, цей модуль відіграє вирішальну роль у посиленні безпеки мережі шляхом ідентифікації потенційних загроз у режимі реального часу. Було опрацьовано кілька вибірок аномального трафіку та отримано низку результатів навчання. Середня ентропія, дисперсія, довірчий інтервал, максимальний довірчий інтервал та мінімальний довірчий інтервал були отримані шляхом статистичного аналізу (рисунок 2).

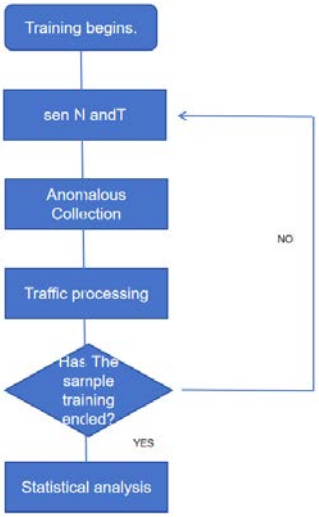

Рис. 2. Блок-схема процесу навчання на вибірках аномального трафіку

Статистичний аналіз результатів вибірки нормального трафіку дозволяє отримати середню ентропію трафіку, дисперсію, довірчий інтервал, максимальний довірчий інтервал та мінімальний довірчий інтервал. Статистичний аналіз результатів вибірки аномального трафіку показує середню ентропію аномального трафіку, дисперсію, довірчий інтервал, максимальний довірчий інтервал та мінімальний довірчий інтервал.

Аналіз швидкостей потоку, як нормальних, так і аномальних, може виявити важливі відмінності в даних. Порівнюючи мінімальний довірчий інтервал нормального потоку з максимальним довірчим інтервалом аномального потоку, можна встановити порогове значення. Відмінність слугує орієнтиром для розмежування нормальної та аномальної швидкості потоку. Хоча будь-яке значення в межах цього інтервалу потенційно може бути використане як поріг, зазвичай доцільно вибирати значення вище максимального довірчого інтервалу аномального потоку як порогове. Такий підхід забезпечує більш точне розмежування нормальних та аномальних швидкостей потоку, що дозволяє краще відстежувати дані потоку та управляти ними.

Експерименти проводилися на віртуальній машині з Ubuntu 22.04. Емулятор мережі Mininet та програмний комутатор Open vSwitch необхідно налаштувати на одній віртуальній машині з Ubuntu 22.04, тоді як контролер Ryu слід встановити на окремій віртуальній машині, що також працює під управлінням Ubuntu 22.04. Така конфігурація забезпечує оптимальну продуктивність і сумісність між пристроями в мережі.

Емулятор мережі Mininet є ідеальною платформою для моделювання топології мережі та генерації трафіку. Для цього використовується власний код програми. За допомогою Mininet було налаштовано власну топологію, тип комутації, версію протоколу OpenFlow, а також параметри підключення до IP-адреси та порту комп'ютера керування. Одночасно було розгорнуто інфраструктуру та управління SDN, а також завершено розробку власного додатка для цього специфічного середовища. Експериментальна топологія базується на скрипті, що імітує мережу в середовищі Mininet.

Експерименти проводилися з використанням часових вікон тривалістю 5 секунд, 10 секунд та 15 секунд. Середній інтервал становить 5, 10 і 15 секунд, а надходження пакетів підпорядковується розподілу Пуассона. Генерація аномального трафіку має свої часові межі та виконує свою функцію під час тестування.

Після незначної модифікації коду було налаштовано контроль над джерелами відправлення пакетів у мережі. У процесі цієї вторинної розробки було реалізовано наступні корисні функції:

– загалом, уся статистична інформація передається та збирається в режимі реального часу;

– збір статистики часу надходження пакетів. Раптовий наплив пакетів (пікові навантаження) додає хаосу, ускладнюючи аналіз патернів передачі даних та поведінки мережевого трафіку;

– за допомогою рівняння розподілу Пуассона визначається ймовірність надходження точної кількості пакетів у межах заданого часового проміжку на основі загального обсягу трафіку;

– формула інформаційної ентропії обчислює ентропію трафіку в конкретному часовому вікні, вказуючи на ймовірність перевантаження або аномалії. Числове представлення допомагає зрозуміти патерни трафіку та оптимізувати інфраструктуру для забезпечення ефективного потоку даних.

Етап тестування має включати три серії експериментів. Перша стратегія атаки передбачає підробку (спуфінг) IP-адреси джерела для атаки на справжню цільову IP-адресу машини в межах мережі клієнта. Другий підхід полягає у підробці IP-адреси джерела та фальсифікації цільової IP-адреси на основі топології мережі клієнта. Успішна реалізація цих стратегій може призвести до згубних наслідків для цільової системи. Третя стратегія атаки є комбінацією перших двох. Для цих трьох різних стратегій обчислюється нормальна швидкість потоку та рівень помилок виявлення.

Часове вікно поділяється на інтервали по 5, 10 та 15 секунд. Потім комутатор надсилає пакети даних до контролера на основі цих інтервалів, що забезпечує ефективну передачу даних та управління ними (рисунок 3).

Як показано на рисунку 3, при тривалості часового вікна 5 секунд та 10 секунд розподіл швидкості вхідних пакетів на контролері є відносно стабільним і близьким до трьох умов, необхідних для аналізу за теорією розподілу Пуассона. У межах 10-секундного інтервалу в деяких суміжних часових вікнах зміна інформаційної ентропії є відносно невеликою. Відповідно, часове вікно, визначене для імітаційного тестування цього методу виявлення, становить 10 секунд.

Під час вимірювання розподілу мережевого трафіку розмір часового вікна є вирішальним фактором для врахування інформаційної ентропії та невизначеності в запропонованій схемі. Зазвичай часове вікно ретельно підбирається для оптимізації результатів. У проведеному експерименті було попередньо вибрано п'ять різних розмірів часових вікон на основі стабільності розподілу потоку пакетів у кількох послідовних вікнах. Згодом було обчислено значення інформаційної ентропії, щоб оцінити ефективність обраних часових вікон для точного вимірювання розподілу мережевого трафіку.

Шляхом налаштування розміру та тривалості часового вікна трафік можна класифікувати як нормальний або аномальний. Статистичний аналіз навчальних тестових даних дозволяє визначити порогове значення ентропії швидкості потоку. Цей метод допомагає розрізняти звичайні патерни трафіку та потенційні аномалії, підвищуючи безпеку та ефективність мережі.

Десять навчальних серій із нормальним трафіком вимірювалися протягом п'яти періодів, кожен з яких тривав 10 секунд, рисунки 4, 5.

Відповідно було розраховано результати статистичного аналізу ентропії для 10 наборів нормальної та аномальної швидкості потоку.

Визначено стандартне відхилення, довірчий інтервал (95% довірчий інтервал), а також верхню та нижню межі довірчого інтервалу. На основі порівняння нижньої межі довірчого інтервалу (мінімуму) для нормальної швидкості потоку та верхньої межі довірчого інтервалу (максимуму) для аномальної швидкості потоку можна встановити відповідне порогове значення на рівні 0.53. Значення слугує надійним індикатором для розмежування цих двох типів трафіку.

У дослідженні розглядалися коефіцієнт виявлення та рівень помилок для аналізу аномальних швидкостей потоку за трьох різних стратегій атак. Під час експериментів на платформі моделювання оцінювалися показники виявлення та помилкові спрацьовування для кожної стратегії. У рамках цього дослідження було визначено розрахунок коефіцієнта виявлення DR, що покращує розуміння аномальних потоків у різних сценаріях атак і демонструє ефективність стратегій виявлення.

Для кількісної оцінки ефективності виявлення трафіку атак використовуються показники TP та FN. Показник TP відображає кількість правильно ідентифікованих вибірок трафіку атаки, тоді як FN позначає вибірки атак, які були пропущені системою під час оцінювання.

Показник FP позначає кількість вибірок нормального потоку, які були хибно розпізнані як

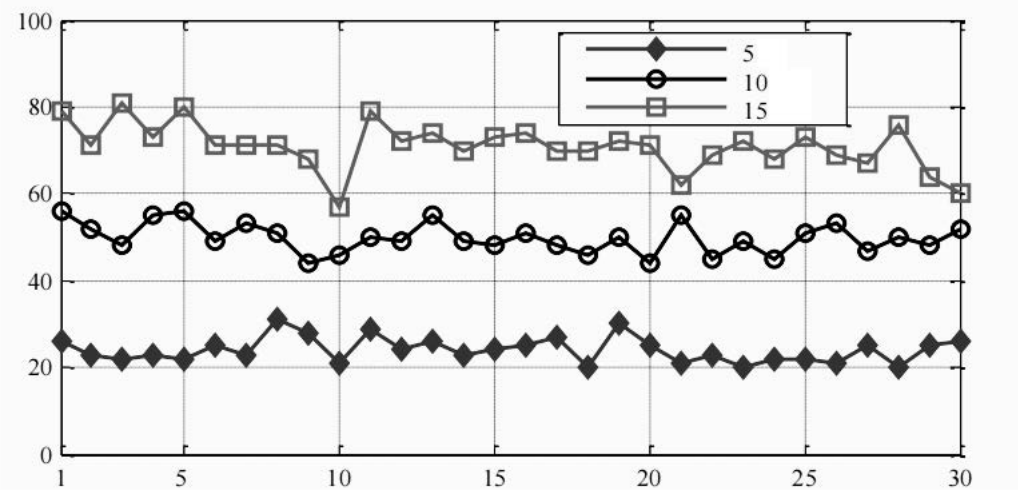

Рис. 3. Часове вікно

Time	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
Number of	50	52	53	48	50	44	47	48	58	45
Entropy	0.78979					0.75881				
Time	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20
Number of packages	51	44	45	42	47	58	56	56	53	53
Entropy value	0.78064					0.76706				
Time	T21	T22	T23	T24	T25	T26	T27	T28	T29	T30
Number of	54	52	52	52	58	58	57	54	52	52
Entropy	0.76627					0.75727				
Time	T31	T32	T33	T34	T35	T36	T37	T38	T39	T40
Number of	54	52	58	57	56	47	47	57	44	50
Entropy	0.76156					0.72570				
Time	T41	T42	T43	T44	T45	T46	T47	T48	T49	T50
Number of packages	57	58	58	58	54	50	50	50	51	49
Entropy value	0.76628					0.80804				

Рис. 4. Звіт щодо нормального потоку

Time	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
Number of	42	52	34	48	50	22	47	31	31	45
Entropy	0.78979					0.75881				
Time	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20
Number of packages	23	44	34	42	47	34	31	31	53	34
Entropy value	0.48064					0.21706				
Time	T21	T22	T23	T24	T25	T26	T27	T28	T29	T30
Number of	23	52	43	52	58	58	23	2	52	21
Entropy	0.56627					0.75727				
Time	T31	T32	T33	T34	T35	T36	T37	T38	T39	T40
Number of	21	21	58	57	56	47	32	57	44	50
Entropy	0.73120					0.64210				
Time	T41	T42	T43	T44	T45	T46	T47	T48	T49	T50
Number of packages	57	58	58	23	54	50	23	50	51	49
Entropy value	0.26234					0.23430				

Рис. 5. Дані аномального потоку

атака, а TN позначає кількість правильно ідентифікованих вибірок нормального потоку.

Експериментальні результати демонструють, що метод виявлення DDoS-атак на контролер SDN із використанням інформаційної ентропії вищого порядку забезпечує кращі показники виявлення та знижує рівень помилок для різних стратегій атак. Інноваційний підхід пропонує надійне рішення для ефективної та дієвої боротьби з кіберзагрозами в системах мережевої безпеки.

Метод виявлення ефективно долає обмеження підходів, що базуються виключно на інформаційній ентропії IP-адрес призначення або IP-адрес джерела, і може широко застосовуватися проти різноманітних стратегій зловмисників. Крім того, цей метод дозволяє додатково інтегрувати ознаки DDoS-атак у контролер SDN та ефективно виявляти атаки, спрямовані безпосередньо на нього.

Експериментальні результати показують, що метод виявлення DDoS-атак на контролер

SDN, який використовує інформаційну ентропію вищого порядку, забезпечує вищий рівень виявлення та зменшує кількість помилок обчислень для різних стратегій атак. Цей підхід пропонує надійне рішення для ефективної та дієвої боротьби з кіберзагрозами в застосунках мережевої безпеки. Метод захисту допомагає фільтрувати різноманітний трафік атак, одночасно запобігаючи DDoS-атакам на контролер.

Порогове значення є більш гнучким і доцільним, ніж середній розподіл.

Метод експоненційного згладжування використовує кількість отриманих повідомлень *Packet-In* у різні часові інтервали для точного прогнозування стану та навантаження контролера. Аналізуючи параболічний тренд, виявлений у повідомленнях *Packet-In*, як надійний метод можна обрати потрійне експоненційне згладжування. Метод забезпечує прогнозування обсягу інформації *Packet-In*, очікуваної в різні часові вікна. Використовуючи ці стратегії, контролери можуть передбачати та ефективно управляти надходженням даних *Packet-In* для досягнення оптимальної продуктивності. Порогове значення передається на кожен граничний комутатор через канал зв'язку між контролером і комутатором. Граничний комутатор управляє повідомленнями із запитами, що надсилаються до контролера, на основі динамічного управління пороговими значеннями.

Конкретні кроки методу динамічного вибору порогового значення на основі експоненційного згладжування є такими:

– налаштування параметрів. Налаштування контролера після моделювання експоненційного згладжування для комутатора та вибір відповідного оптимального параметра згладжування;

– прогнозування базових значень для різних граничних комутаторів. Контролер виконує експоненційне згладжування на основі формули потрійного експоненційного згладжування, яка підраховує кількість повідомлень, надісланих від різних граничних комутаторів із запитом на правила таблиці потоків для кожного часового вікна, та прогнозує згладжене значення для наступного часового вікна;

– встановлення порогових значень. Контролер встановлює порогове значення для повідомлень із запитами кожного граничного комутатора на основі відсотка повідомлень, відправлених цим комутатором у попередньому часовому вікні, згладженого прогнозованого значення для наступного часового вікна та загальної кількості запитів до контролера;

– динамічне коригування. Контролер коригує пороги запитів для різних граничних комутаторів у режимі реального часу за допомогою протоколів зв'язку, забезпечуючи ефективний розподіл ресурсів на рівні інфраструктури без високих накладних витрат.

Експериментальне моделювання SDN переважно включає симуляцію мережевої платформи SDN, симуляцію контролера та моделювання мережевого трафіку.

Для генерації нормального експериментального трафіку використовується команда iperf, що запускається за допомогою shell-скрипта, тоді як аномальний трафік створюється за допомогою інструмента hping3. Методи слугують для перевірки продуктивності мережі та виявлення потенційних вразливостей. DDoS-атака на контролер SDN моделювалася за допомогою методу SYN Flood.

Тестове середовище побудоване з використанням двох віртуальних машин наведено на рисунок 6.

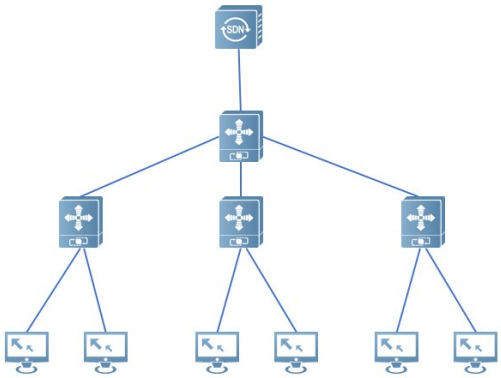

Рис. 6. Карта спеціальної топології для експерименту із захисту мережі

Було виконано моделювання на основі експоненційного згладжування, за результатами якого кінцеві параметри згладжування були визначені як 0.14 та 0.27 відповідно.

Під час експерименту після імітації DDoS-атак було проведено вимірювання кількості повідомлень *Packet-In*, отриманих контролером від комутатора, кількості правил таблиці потоків, переданих на комутатор, а також рівня втрати пакетів для звичайного UDP-трафіку в кожному часовому вікні для кількох груп без використання політик захисту.

У межах цього дослідження було оцінено різні стратегії захисту разом із кількістю правил таблиці потоків, надісланих контролером на комутатор. Крім того, під час експерименту було змодельовано рівень втрати пакетів нормального

UDP-трафіку після DDoS-атаки на контролер. Метою було визначити ефективність різних стратегій у пом'якшенні наслідків таких атак.

Результати продемонстрували різні рівні успішності в захисті мережевої інфраструктури та мінімізації збоїв, спричинених зловмисною діяльністю. Було проведено порівняльний аналіз експериментальних результатів на основі двох різних стратегій.

У цьому експерименті DDoS-атаки на контролер розглядалися у двох різних ситуаціях: за наявності заходів захисту та за їхньої відсутності.

Контролер під час симуляції оцінює дані вхідних пакетів від комутаторів, що дозволяє йому ефективно керувати мережевим трафіком. Тести підтверджують ефективність цього процесу за різних умов, що гарантує надійну роботу системи.

Застосовуючи стратегію захисту, граничні комутатори можуть оцінювати надійність пакетів за допомогою встановленого порогу, відправляючи до контролера лише надійні повідомлення, незважаючи на наявність трафіку атаки. Цей підхід підвищує безпеку та ефективність мережі, оскільки комутатори надають пріоритет надійній передачі даних. Такий механізм оцінки в реальному часі забезпечує цілісність системи та мінімізує збої, спричинені потенційними загрозами. Нормальна IP-адреса джерела знаходиться в таблиці історії надійних IP-адрес і її трафік передається контролеру, тоді як IP-адреса джерела потоку атаки в ній відсутня. Система відстежує та зберігає IP-адреси, залучені до атак, знижуючи рівень довіри до пакетів, надісланих із цих адрес. Позначаючи підозрілі IP-адреси та фільтруючи їхній трафік, система ефективно нейтралізує потенційні загрози. Проактивний захід допомагає захиститися від зловмисних атак і гарантує безпеку мережі. Експериментальні дані щодо захисту від атак показують, що коли контролер зазнає DDoS-атаки, розроблена стратегія ефективно фільтрує велику кількість хибних повідомлень і запобігає перевантаженню контролера величезним обсягом шкідливого трафіку.

Без політики захисту DDoS-атака може легко перевантажити контролер в 11-му часовому вікні, що призведе до різкого збільшення втрати пакетів для нормального мережевого трафіку. Вкрай важливо мати механізми захисту для запобігання таким збоям. Під час 14-го часового вікна рівень втрати пакетів нормального трафіку в мережі досягає 100%. Після вжиття заходів захисту рівень втрати пакетів у часових вікнах 11, 12 та 13 залишається низьким (у межах норми), нормальна передача UDP-трафіку підтримується в наступних часових вікнах, а рівень втрати пакетів падає до 0.

Коли контролер зазнає DDoS-атаки, більша частина трафіку атаки інкапсулюється в пакети, надіслані до контролера, які вимагають створення нових правил таблиці потоків. Ці запити не лише споживають величезні обсяги ресурсів пропускної здатності контролера, але й змушують його помилково надсилати шкідливі правила на комутатор. Таким чином, під час обробки нормального UDP-трафіку контролеру вже не вистачає ресурсів для встановлення правил передачі, і він відкидає багато легітимних UDP-пакетів. Політика захисту дозволяє контролеру забезпечити безперебійну обробку UDP-трафіку шляхом передачі правил маршрутизації на комутатор на основі вхідних повідомлень із запитами, гарантуючи стабільну роботу мережі. Саме тому рівень втрати пакетів значно знизився після вжиття заходів захисту.

Ефективність захисту контролера SDN від DDoS-атак можна оцінити за трьома ключовими показниками:

− кількість вхідних пакетів, отриманих контролером від комутатора;

− кількість правил таблиці потоків, надісланих на комутатор;

− рівень втрати пакетів для нормального UDP-потоку.

Використовуючи динамічні пороги та рівні довіри до IP-адрес джерела, контролер може успішно відфільтровувати потоки DDoS-атак, згенеровані такими інструментами, як hping3. Цей проактивний підхід захищає контролер від перевантаження під час атак, дозволяючи йому продовжувати надавати нормальні послуги. Постійно відстежуючи та коригуючи ці порогові значення, контролер може ефективно звести нанівець вплив DDoS-атак на свою роботу. Отже, запропонований у цьому розділі метод надійно та ефективно захищає контролер SDN.

Висновки. Проведене дослідження дозволило розробити та всебічно обґрунтувати адаптивний метод захисту контролера програмно-конфігурованих мереж від розподілених атак на відмову в обслуговуванні. Наукова новизна підходу полягає у синергії використання інформаційної ентропії вищого порядку та статистичної моделі розподілу Пуассона, що забезпечує високу точність детектування аномалій навіть за умов складних стратегій атак із використанням підробки IP-адрес.

Експериментальна перевірка на базі емулятора Mininet та контролера Ryu підтвердила, що часове вікно тривалістю 10 секунд та порогове значення ентропії 0,53 є оптимальними параметрами для стабільної ідентифікації шкідливого трафіку. Впровадження механізму динамічного керування порогами на основі експоненційного згладжування разом із системою оцінки кредитів довіри до джерел дозволило перенести частину обчислювального навантаження на граничні комутатори. Це стратегічне рішення забезпечило ефективну фільтрацію повідомлень Packet-In, що критично важливо для запобігання перевант-

таженню центрального процесора контролера та каналів зв'язку.

Аналіз результатів моделювання продемонстрував ефективність запропонованої методики у сценаріях із активованим захистом рівень втрати пакетів легітимного трафіку знизився до нуля, тоді як у незахищеній мережі атака призводила до повної відмови в обслуговуванні. Таким чином, розроблений метод не лише підвищує рівень кібербезпеки SDN-інфраструктури, але й гарантує безперервність надання мережевих послуг у реальному часі, що робить його перспективним для впровадження у сучасних корпоративних та хмарних мережах.

Список літератури:

1. Choi W., Pandey S. Kim J. Detecting Cybersecurity Threats for Industrial Control Systems Using Machine Learning. *IEEE Access.* 2024. № 12. Pp. 153550-153563. https://doi.org/10.1109/ACCESS.2024.3478830

2. Яровий К.О., Гончар Л.В., Бабаян Д.П. Інформаційні системи і технології як невід'ємна частина в управлінні підприємством. *Інноваційна економіка*. 2021. № 7-8. С. 119-23. https://doi.org/10.37332/2309-1533.2021.7-8.16

3. Барковська О.Ю., Ні Я.С., Янковський О.А., Романенко А.О., Перетяка Є.О. Модель системи автоматизованого навантажувального тестування програмних застосунків із використанням методів штучного інтелекту. *Інформаційно-керуючі системи на залізничному транспорті.* 2025. № 1(30). С. 47-58. https://doi.org/10.18664/ikszt.v30i1.326699

4. Fedorchenko V., Yeroshenko O., Shmatko O., Kolomiitsev O., Omarov M. Password hashing methods and algorithms on the .Net platform. *Advanced Information Systems*. 2024. № 8(4). Pp. 82–92. https://doi.org/10.20998/2522-9052.2024.4.11

5. Barkovska O., Ruban I., Tymoshenko D., Holovchenko O., Yankovskyi O. Research on mobile machine learning platforms for human gesture recognition in human-machine interaction systems. *Technology Audit and Production Reserves*. 2025. №2(2(82). Pp. 6–14. https://doi.org/10.15587/2706-5448.2025.325423

6. Idris M., Syarif I., Winarno I. Web Application Security Education Platform Based on OWASP API Security Project. *EMITTER International Journal of Engineering Technology.* 2022. №10(2). Pp. 246-261. https://doi.org/10.24003/emitter.v10i2.705

7. Barkovska O. Двофакторна автентифікація на основі методу KWS та голосової верифікації. *Сучасний стан наукових досліджень та технологій в промисловості*. 2025. № 3(33). С. 5–18. https://doi.org/10.30837/2522-9818.2025.3.005

8. Федорченко В.М., Єрошенко О.А. Застосування алгоритмів штучного інтелекту для моделювання загроз інформаційних систем. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки».* 2025. Т.6 (75). Ч. 2. С. 384-391. https://doi.org/10.32782/2663-5941/2025.6.2/52

Yeroshenko O.A., Fedorchenko V.M., Partyka S.O., Pyvovarova D.I. HIGHER-ORDER INFORMATION ENTROPY-BASED DDOS ATTACK DETECTION METHOD FOR SDN CONTROLLER

The article is devoted to solving the urgent problem of ensuring the security of Software-Defined Networks (SDN), specifically protecting the network control plane from Distributed Denial of Service (DDoS) attacks. The unique architecture of SDN, which separates the control plane from the data plane, makes the centralized controller a critical point of failure and a primary target for cyber-attacks. Overloading the Packet-In resource leads to total degradation of the entire network infrastructure.

The paper analyzes the shortcomings of existing statistical analysis methods, which typically focus only on the set of IP addresses without considering dynamic temporal factors, making them vulnerable to sophisticated attack strategies such as intelligent spoofing. The authors propose an enhanced DDoS attack detection method based on the use of higher-order information entropy and a Poisson distribution statistical model. The core of the method lies in the precision analysis of packet flow rates within fixed time windows. Modeling the request arrival process as a Poisson process allows for more accurate identification of anomalous traffic fluctuations: under normal conditions, entropy remains consistently high due to the statistical randomness of flows, whereas during an attack, it drops sharply as a result of artificial traffic concentration on specific nodes.

Experimental validation of the method was conducted using a distributed topology in the Mininet emulator, Open vSwitch, and the Ryu controller. Simulation results confirmed that the proposed approach provides higher detection accuracy and a significantly lower computational error rate for various attack strategies compared to traditional solutions. It was established that a 10-second time window is optimal for stable anomaly detection. Additionally, an implemented "trust credit" system for source IP addresses effectively filters malicious traffic at the edge switch level, preserving scarce controller resources for legitimate requests. This ensures high availability and resilience of the network infrastructure even under intensive cyber-influence.

Keywords: *Software-Defined Networks, SDN controller, DDoS attacks, information entropy, poisson distribution, cybersecurity, time window, exponential smoothing.*

Дата першого надходження статті до видання: 27.03.2026
Дата прийняття статті до друку після рецензування: 24.04.2026
Дата публікації (оприлюднення) статті: 19.05.2026