УДК 004.415.2
DOI https://doi.org/10.32782/2663-5941/2025.2.1/24

Шпур О. М.
Національний університет «Львівська політехніка»

Гаврилів Т. М.
Національний університет «Львівська політехніка»

ГІБРИДНИЙ ПІДХІД ДО ВИЯВЛЕННЯ КІБЕРЗАГРОЗ У ТЕЛЕКОМУНІКАЦІЙНИХ ІОТ МЕРЕЖАХ ІЗ ВИКОРИСТАННЯМ ЛЕГКИХ ML-МОДЕЛЕЙ

У статті пропонується гібридний підхід до ефективного виявлення та запобігання DDoS-атакам, який в умовах швидко зростаючої кількості IoT-пристроїв, дозволяє здійснювати виявлення аномалій без значного навантаження на пристрої та мережу в цілому. Його основою є розроблення алгоритму виявлення аномалій, який дозволяє комплексно підійти до оцінки та аналізу мережевого трафіку, використовуючи легкі ML модулі для забезпечення своєчасного виявлення атак. Запропонований підхід використовує багаторівневу модель системи управління, що включає рівень доступу, Edge-аналіз на серверах AWS Greengrass, SDN та хмарний штучний інтелект та дозволяє проводити аналіз трафіку ближче до джерела, мінімізуючи затримки та навантаження на центральні сервери. На Edge-рівні здійснюється перший етап аналізу за допомогою легких методів машинного навчання, серед яких ентропійний аналіз, евристичний аналіз SYN-запитів та класифікація трафіку за допомогою моделі Isolation Forest. Ці методи дозволяють ефективно ідентифікувати потенційні DDoS-атаки, спираючись на статистичні показники, такі як концентрація трафіку, частота SYN-запитів та зміни в загальному обсязі трафіку. У випадку виконання хоча б однієї з умов – чи низька величина ентропії з однієї IP адреси, чи велика кількість SYN-запитів та їх сплески – алгоритм надсилає повідомлення про блокування даної IP на рівень управління. Важливим етапом є інтеграція з керуючим рівнем SDN, де використовуються алгоритми для оперативного управління мережевим трафіком на основі отриманих результатів аналізу. SDN-контролер може реалізовує політику блокування або обмеження трафіку з даної IP-адреси, що дозволяє миттєво реагувати на виявлені загрози. Система автоматично генерує сигнал тривоги та застосовує політики захисту за умови, коли два з трьох методів виявляють аномалію. Це дозволяє значно зменшити час реакції на загрози та забезпечити ефективний захист у реальному часі. Крім того, на хмарному рівні за допомогою технологій Federated Learning і Reinforcement Learning здійснюється оптимізація політик управління та адаптація системи до нових типів атак.

Ключові слова: *DDoS-атаки, виявлення аномалій, легкі ML модулі, IoT мережі, AWS Greengrass, аналіз мережевого трафіку.*

Постановка проблеми. Сучасні телекомунікаційні системи є фундаментальною складовою критичної інфраструктури держав та бізнесу, забезпечуючи надійну комунікацію, передачу даних і підтримку роботи Інтернету речей (IoT). Стрімке зростання кількості IoT-пристроїв – за прогнозами, понад 85 мільярдів до 2026 року – призводить до появи нових можливостей та водночас збільшує ризики кібератак [1]. Серед таких загроз особливе місце займають розподілені атаки на відмову в обслуговуванні (DDoS), що використовують вразливості IoT-пристроїв для генерації масового шкідливого трафіку. Відомим прикладом таких атак є атака Mirai, яка спричинила серйозні перебої в роботі глобальних інтернет-сервісів [4].

Незважаючи на значну кількість розроблених методів виявлення і запобігання кіберзагрозам, сучасні рішення демонструють низку суттєвих недоліків, серед яких недостатня точність, висока затримка реакції та значні витрати на обчислення. Тому актуальною залишається задача розробки нових підходів, здатних ефективно функціонувати в умовах реального часу та обмежених ресурсів IoT.

Аналіз останніх досліджень і публікацій. Сучасні методи виявлення кіберзагроз у телекомунікаційних системах переважно базуються на сигнатурному, поведінковому та гібридному аналізах. Сигнатурні методи є ефективними для виявлення відомих атак, проте нездатні ідентифікувати нові

загрози («атаки нульового дня») [1]. Поведінкові методи, що аналізують відхилення від звичайних режимів роботи систем, ефективніші у виявленні нових атак, але характеризуються високою частотою помилкових спрацьовувань [3]. Гібридні методи поєднують переваги двох попередніх підходів, застосовуючи алгоритми машинного навчання для зменшення помилок та підвищення швидкості реагування [2]. Однак, їх практичне впровадження ускладнюється необхідністю великих обчислювальних ресурсів, які недоступні для багатьох IoT-пристроїв [5, 6].

Іншою суттєвою проблемою є затримка у виявленні атак, особливо для мереж із програмно-визначеною архітектурою (SDN). Великі обсяги даних, що передаються на центральні контролери SDN, спричиняють значні затримки у реакції на загрози. Перспективним напрямком є перенесення задач аналітики на край мережі (Edge computing), що дозволяє оперативно виявляти загрози ближче до джерела їх виникнення [6, 7].

У відповідь на вирішення цієї проблеми, було проведено багато досліджень щодо розробки механізмів захисту від атак DDoS. Серед них методи засновані на ентропії відіграють вирішальну роль. Як правило, ентропійні методи виявляють аномальну поведінку шляхом аналізу розподілу та зміни мережевого трафіку, тим самим ідентифікуючи та захищаючи від DDoS-атак [8–11]. Лі (Li) та ін. [12] запропонували метод виявлення DDoS-атак на основі φ-ентропії для раннього виявлення атак у мережах SDN. Завдяки регулюванню параметрів φ-ентропії цей метод підсилює відмінності між нормальними та ненормальними характеристиками трафіку, полегшуючи виявлення атак на ранніх стадіях формування трафіку DDoS. Анчал (Anchal) та ін. [13] використовували ентропію Реньї для виявлення атак DDoS, підвищуючи точність виявлення та ефективність шляхом вибору відповідних порогів.

Методи, засновані на цінності довіри, також відіграють важливу роль у виявленні атак DDoS. Ці методи оцінюють поведінку та історію взаємодії вузлів, щоб визначити їхню надійність, тим самим ідентифікуючи та захищаючи від шкідливих атак [14, 15]. Наприклад, Магдіч (Magdich) та ін. [16] запропонував модель управління довірою, яка не тільки ідентифікує довірені вузли, але також використовує методи машинного навчання для виявлення та запобігання зловмисним атакам шляхом вивчення характеристик поведінки зловмисного вузла. В іншому дослідженні Вафа (Wafa) та ін. [17] запропонував модель управління довірою, яка аналізує поведінку взаємодії вузлів і призначає розумні значення довіри для виявлення атак. Крім того, Хуан (Juan) та ін. [18] використовували математичні моделі та статистичний аналіз для виявлення аномального трафіку, тоді як Баскар (Baskar) [19] поєднав методи аналізу великих даних для точної ідентифікації та захисту від складних DDoS-атак.

Незважаючи на те, що ці методи показали чудову продуктивність у виявленні DDoS-атак, вони все ще мають деякі недоліки щодо поточних складних типів DDoS-атак [20]. Наприклад, використання фіксованих порогів може бути недостатньо гнучким при роботі з динамічними DDoS-атаками, що призводить до зниження ефективності виявлення. Методи, запропоновані в [12, 13], недостатньо точні при атаках з низькою щільністю. Так само методи, описані в [16, 17], не реагують швидко в динамічних мережевих середовищах. Крім того, оскільки методи атак продовжують розвиватися, ці методи потребують постійного оновлення та вдосконалення, щоб адаптуватися до нових проблем безпеки мережі.

В останні роки методи глибокого навчання поступово передовими для дослідників у галузі DDoS [21–23]. Крім того, машинне навчання – це метод, здатний автоматично вивчати моделі з даних і робити прогнози. Використання глибоких нейронних мереж для виявлення кібератак ускладнюється їх значними обчислювальними витратами, що робить їх неефективними для IoT-пристроїв із обмеженими ресурсами. Оптимізація таких мереж шляхом застосування легких архітектур, методів компресії моделей, transfer learning та federated learning є перспективним шляхом подолання цієї проблеми [5, 6, 8].

Для ефективного захисту сучасних телекомунікаційних систем, особливо в умовах IoT, необхідна адаптація існуючих методів до реальних умов функціонування пристроїв, враховуючи їх динамічність, різноманітність і обмеженість ресурсів [7, 8].

Постановка завдання. Таким чином, метою роботи є розроблення та дослідження ефективної архітектури телекомунікаційної системи для виявлення і запобігання DDoS-атакам в умовах функціонування Інтернету речей (IoT). Особлива увага приділяється розробці методу для раннього виявлення аномалій у трафіку IoT-пристроїв за допомогою легких машинних навчальних моделей, що дозволить забезпечити оперативне реагування на кіберзагрози, зокрема в умовах обмеженості програмно-апаратних ресурсів пристроїв мережі.

Виклад основного матеріалу. Запропонована архітектура телекомунікаційної системи (ТКС)

є складним багаторівневим рішенням, орієнтованим на швидке виявлення та ефективне протистояння різноманітним мережевим загрозам, особливо DDoS-атакам. Сучасні IoT-пристрої генерують величезні обсяги трафіку, що вимагає комплексного підходу до його аналізу та обробки. Саме тому у запропонованій системі використовується розподілена архітектура, яка складається з кількох функціонально взаємопов'язаних рівнів (рис. 1):

- Рівень доступу (Access Layer).
- Edge-рівень (AWS Greengrass).
- Рівень керування (SDN Control Plane, контролер Ryu).
- Верхній рівень, що базується на штучному інтелекті (Cloud AI).

Кожен рівень має чітко визначені функції, специфічні алгоритми аналізу й особливий тип інформації, яка збирається, аналізується та передається між рівнями.

Рівень доступу (Access Layer) – найнижчий рівень архітектури, який складається із великої кількості IoT-пристроїв, які забезпечують генерацію первинного трафіку. Ці пристрої, як правило, мають мінімальні обчислювальні можливості, відсутній складний вбудований захист, тому є найбільш вразливими для атак і використання в якості інструментів для реалізації DDoS.

Серед типових пристроїв цього рівня: датчики руху, камери відеоспостереження, датчики температури, освітлення, мобільні термінали, смартфони, сенсорні пристрої розумного дому. Вони

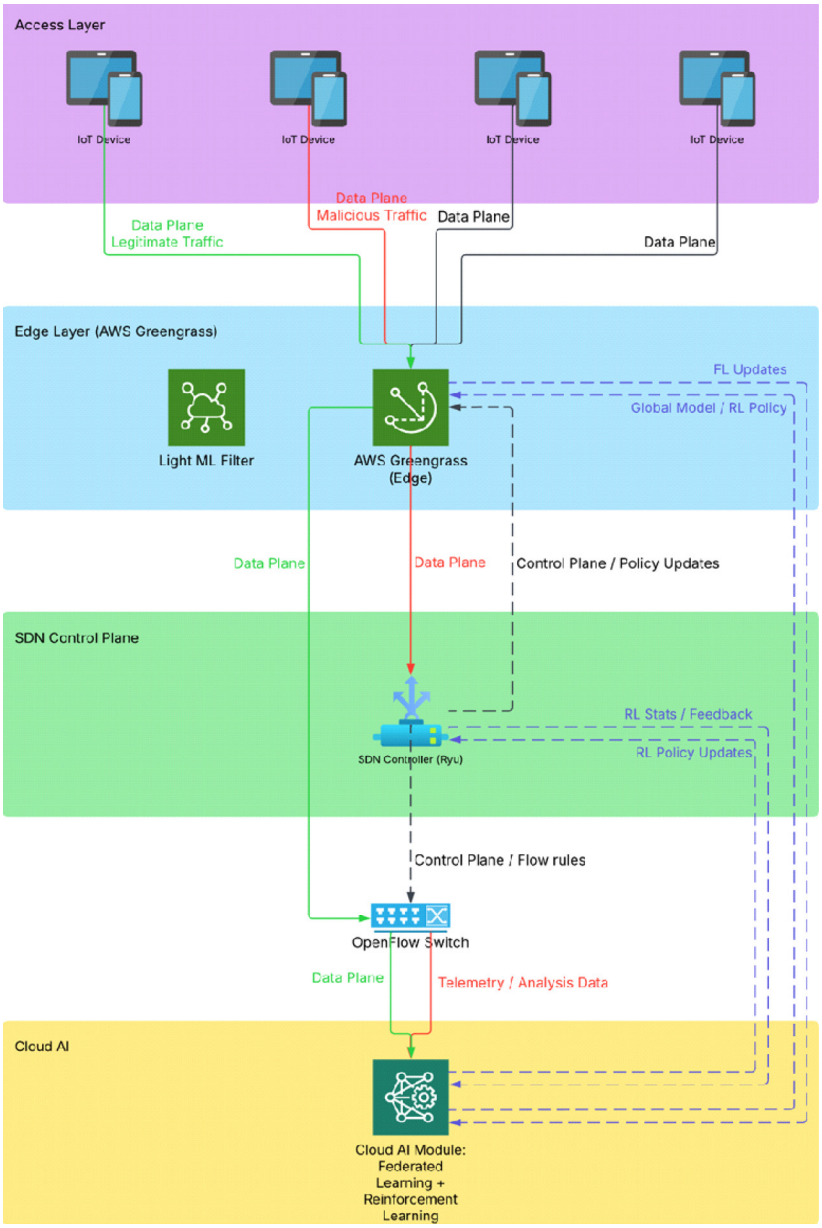

Рис. 1. Архітектура IoT-мережі з системою виявлення аномалій

безперервно передають великий обсяг трафіку, що містить як легітимні, так і потенційно шкідливі пакети. Основними протоколами, які застосовуються на цьому рівні, є TCP, UDP та ICMP, серед яких особливе значення мають TCP SYN-запити, оскільки саме їхня кількість часто використовується зловмисниками при SYN Flood атаках.

Трафік із цього рівня не проходить ніякої аналітики безпосередньо на пристроях. Усі пакети без будь-якої попередньої фільтрації чи класифікації надходять до наступного рівня – Edge-серверів AWS Greengrass.

Edge-рівень є критично важливим компонентом запропонованої архітектури, оскільки саме тут здійснюється перший етап аналізу та фільтрації. На цьому рівні використовуються сервери AWS Greengrass – платформа, яка спеціально призначена для ефективної роботи в умовах обмежених ресурсів. Edge-сервери отримують трафік безпосередньо з IoT-пристроїв, виконують його аналіз та первинну фільтрацію.

На Edge-рівні впроваджується легкий ML-фільтр, який містить у собі декілька аналітичних модулів, зокрема:

- Ентропійний аналіз: дозволяє оцінити концентрацію трафіку за IP-адресами й швидко ідентифікувати DDoS-атаки за їхнім характерним профілем – надмірною концентрацією або надмірною розподіленістю пакетів.
- Евристичний аналіз SYN-запитів: цей модуль орієнтований на швидке виявлення SYN Flood атак шляхом оцінки поточної кількості SYN-запитів та їхнього відхилення від нормального режиму роботи мережі.
- Isolation Forest: легка модель машинного навчання, яка дозволяє класифікувати трафік за набором параметрів як нормальний або аномальний.

Edge-сервер Greengrass виконує ці аналізи кожні 60 секунд (ковзне вікно аналізу), збираючи статистичні дані, серед яких:

- IP-адреси джерел і призначень;
- TCP та UDP порти;
- частота SYN-запитів;
- загальна кількість пакетів;
- розподіл трафіку за типами протоколів.

Якщо Edge-рівень виявляє очевидну аномалію, він формує сигнал тривоги, до якого додаються метадані (тип атаки, IP-порушники, статистичні показники трафіку). Цей сигнал передається до наступного рівня – SDN Control Plane, на контролер Ryu, який має повноваження впроваджувати оперативні правила управління трафіком.

Рівень керування (SDN Control Plane, Ryu) є центральним координаційним рівнем, де SDN-контролер Ryu отримує інформацію з Edge-рівня, аналізує її та ухвалює рішення щодо подальших дій у мережі. Контролер Ryu є гнучким рішенням, написаним мовою Python, що дозволяє йому ефективно взаємодіяти з різними аналітичними системами.

Отримавши сигнал від Edge-рівня, контролер визначає тип загрози і застосовує правила керування потоками (блокування трафіку, обмеження швидкості, зміна маршрутів), використовуючи протокол OpenFlow та мережеві комутатори.

Крім цього, SDN-контролер передає на верхній рівень (Cloud AI) статистичні дані щодо ефективності застосованих політик і отримує від нього рекомендації щодо їх вдосконалення.

Cloud AI: Federated Learning ma Reinforcement Learning – є найвищим рівнем розробленої архітектури. Це хмарне середовище, в якому реалізуються складні методи штучного інтелекту: Federated Learning (FL) і Reinforcement Learning (RL). Federated Learning дозволяє створювати глобальну ML-модель на основі агрегування оновлених ваг локальних моделей із Edge-рівня. Це дає змогу Edge-вузлам зберігати актуальність моделей без передачі чутливих даних до хмари.

Reinforcement Learning, натомість, аналізує ефективність політик, застосованих контролером Ryu, і на основі зворотного зв'язку виробляє оптимальні стратегії управління трафіком. Сформовані політики повертаються до SDN-контролера та Edge-серверів для їх впровадження.

Для пропонованої архітектури функціонування IoT мережі ми розробили алгоритм роботи легких ML-модулів для виявлення аномалій на EDGE-серверах. Ефективне виявлення атак повинно здійснюватися якомога ближче до джерела трафіку, щоб уникнути зайвого навантаження на хмарні та центральні сервери. Саме з цією метою розроблений алгоритм виявлення аномалій працює безпосередньо на AWS Greengrass. AWS Greengrass є проміжним (Edge) вузлом, який має достатні обчислювальні можливості для початкової аналітики, проте має обмеження щодо ресурсів процесора та пам'яті. Враховуючи ці обмеження, алгоритм був спеціально розроблений для максимально ефективного використання ресурсів. Він включає три взаємопов'язані методи аналізу:

- ентропійний аналіз розподілу пакетів за IP-адресами;
- евристичний аналіз частоти SYN-запитів та різких змін у кількості трафіку;

• класифікація за допомогою легкої ML-моделі Isolation Forest.

Ентропійний аналіз розподілу пакетів буде відбуватися за кількісної оцінки неоднорідності розподілу пакетів між IP-адресами. Зазвичай під час DDoS-атак трафік характеризується або надмірною концентрацією (низька ентропія), або надмірною розподіленістю (висока ентропія). В загальному випадку, ентропія Шеннона враховує частку трафіку, що надійшла від IP-адреси p_i та загальну кількість унікальних IP-адрес N, що надіслали пакети за визначений інтервал часу.

$$E = -\sum_{i=1}^{N} p_i \log_2 p_i.$$

Наприклад, якщо за 60 секунд ми отримали 10 000 пакетів, і вони розподілилися таким чином:

• IP-адреса 1: кількість пакетів – 7000; частка p_i – 0.7;

• IP-адреса 2: кількість пакетів – 1500; частка p_i – 0.15;

• IP-адреса 3: кількість пакетів – 1000; частка p_i – 0.1;

• IP-адреса 4: кількість пакетів – 500; частка p_i – 0.05;

Тоді ентропія дорівнюватиме:

$$E = -(0.7 \log_2 0.7 + 0.15 \log_2 0.15 + 0.1 \log_2 0.1 + \\ + 0.05 \log_2 0.05) \approx 1.36.$$

Отримане значення порівнюється з порогом, встановленим на основі історичних даних (наприклад, середня ентропія за тиждень – 3.2, тоді порогове значення береться на 15 % нижче, тобто 2.72). Значення 1.36 значно менше за 2.72, отже є ознакою потенційної атаки. В нашому випадку Edge-сервер кожні 60 секунд буде аналізувати IP-адреси (джерела та призначення); TCP/UDP порти; кількість пакетів за типами протоколів (TCP, UDP, ICMP); загальну кількість SYN-запитів, а також проводиться підрахунок часток пакетів (p_i) для кожної IP-адреси. Далі іде порівняння розрахованих значень із даними отриманими в попередні моменти часу.

Наступним етапом є евристичний аналіз. Він матиме кілька складових. Перша – перевірка кількості SYN-запитів: якщо перевищення середнього значення за попередній тиждень на 25 % і більше, то визначається можливий SYN Flood. Другий – проводиться аналіз різкого зростання трафіку: якщо кількість пакетів перевищує більш ніж вдвічі середнє значення за попередні три інтервали часу, генерується сигнал про виявлення аномалії.

Далі відбуватиметься класифікація за допомогою легкої ML-моделі Isolation Forest. Isolation Forest отримавши значення ентропії, кількості SYN-запитів, загальної кількості пакетів, співвідношення кількості пакетів поточного інтервалу до середнього за попередні три дні. Isolation Forest оцінює ці показники й видає оцінку аномалії (score). Якщо значення score < 0.3 – це свідчить про наявність аномалії.

Якщо хоча б два з трьох методів оцінки (ентропійний аналіз, евристичний аналіз, Isolation Forest) вказують на аномалію, система автоматично:

• надсилає сигнал тривоги на SDN-контролер Ryu;

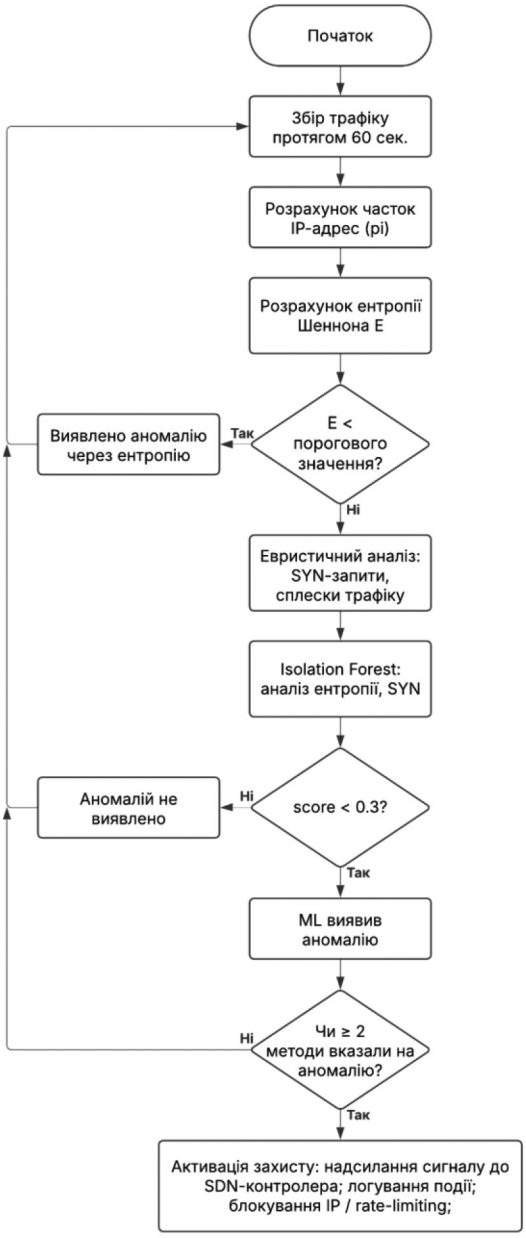

Рис. 2. Блок-схема алгоритму виявлення аномалій на Edge-сервері

• записує детальну інформацію в журнал подій;

• застосовує політики блокування або обмеження трафіку.

Блок-схема розробленого алгоритму наведена на рисунку 2.

Висновки. Проведений аналіз сучасних викликів інформаційної безпеки у сфері телекомунікаційних систем та Інтернету речей (IoT) дозволив визначити ключові проблеми виявлення кіберзагроз, особливо DDoS-атак. Основними недоліками існуючих методів є низька точність виявлення нових атак, високі обчислювальні витрати та затримки реагування у централізованих системах.

Запропоновано багаторівневу архітектуру, яка використовує переваги Edge computing, легкі алгоритми машинного навчання (Isolation Forest, евристичний та ентропійний аналіз) та сучасні підходи Federated Learning і Reinforcement Learning. Це дозволило суттєво зменшити затримку реагування, підвищити точність виявлення атак, особливо низькоінтенсивних (Low-rate) DDoS, та забезпечити ефективну роботу системи в умовах обмежених ресурсів IoT-пристроїв.

Практичне значення запропонованого рішення полягає у високій адаптивності та масштабованості, що дає змогу оперативно реагувати на нові типи кіберзагроз та легко інтегрувати додаткові пристрої чи аналітичні модулі. Подальші дослідження рекомендується зосередити на вдосконаленні алгоритмів машинного навчання та посиленні стійкості систем до інтенсивних і тривалих атак.

Список літератури:

1. Lali M, Mustafa R, Ahsan F, Nawaz M, Aslam W. Performance evaluation of software defined networking vs. Traditional networks. Nucleus. 2017, No. 54(1), pp. 6–22.

2. Douligeris C, Mitrokotsa A. DDoS attacks and defense mechanisms: classification and state-of-the-art. Comput Netw. 2004, No 44(5), pp. 643–666.

3. Turner J. The year of widespread SDN adoption and DDoS attack mitigation, 2017. Available from: https://surl.li/hcrqoy

4. Kavisankar L, Chellappan C. A mitigation model for TCP SYN flooding with IP spoofing. Paper presented at: Proceedings of the 2011 International Conference on Recent Trends in Information Technology (ICRTIT); 2011. pp. 251–256.

5. Lim S, Ha J, Kim H, Kim Y, Yang S. A SDN-oriented DDoS blocking scheme for botnet-based attacks. Paper presented at: Proceedings of the 2014 6th International Conference on Ubiquitous and Future Networks (ICUFN); 2014. pp. 63–68.

6. Dayal N, Srivastava S. Analyzing behavior of DDoS attacks to identify DDoS detection features in SDN. Paper presented at: Proceedings of the 2017 9th International Conference on Communication Systems and Networks (COMSNETS); 2017. pp. 274–281.

7. Chen CC, Chen YR, Lu WC, Tsai SC, Yang MC. Detecting amplification attacks with software defined networking. Paper presented at: Proceedings of the 2017 IEEE Conference on Dependable and Secure Computing; 2017. Taipei, Taiwan. pp. 195–201.

8. Kamolphiwong S., Kamolphiwong T. The design of SDN based detection for distributed denial of service (DDoS) attack. Paper presented at: Proceedings of the 2017 21st International Computer Science and Engineering Conference (ICSEC); 2017. Bangkok, Thailand: IEEE. pp. 1–5.

9. Dayal N., Srivastava S. SD-WAN flood tracer: tracking the entry points of DDoS attack flows in WAN. Comput Netw. 2021; 186:107813.

10. Ryhan Uddin, Sathish A.P. Kumar, Vinay Chamola. Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions. Ad Hoc Networks. 2024; 152(11):103322.

11. Yin C, Zhu Y, Fei J, He X. Collaborative prediction and detection of DDoS attacks in edge computing: A deep learning-based approach with distributed SDN. IEEE Trans Inf Forensics Secur. 2020; 15:4169–4183.

12. Doshi R, Apthorpe N, Feamster N. SmartDefense: A distributed deep defense against DDoS attacks with edge computing. Paper presented at: Proceedings of the ACM SIGCOMM Workshop on IoT Security and Privacy; 2018.

13. Alwarafy A., Al-Thelaya KA, Abdallah M., Schneider J., Hamdi M. Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions. ACM Comput Surv. 2021; 54(5):1–36.

14. Luong NC, Hoang DT, Gong S, Niyato D, Wang P., Liang YC, Kim DI. Detection and prevention of DDoS attacks on edge computing of IoT devices through reinforcement learning. IEEE Internet Things J. 2019; 7(5):4202–4213.

15. Gadze JD, Bamfo-Asante AA, Agyemang JO, Nunoo-Mensah H, Opare KAB. An investigation into the application of deep learning in the detection and mitigation of DDOS attack on SDN controllers. *Technologies*. 2021; 9(1):14.

16. Xie J, Yu FR, Huang T., et al. A survey of machine learning techniques applied to software defined networking (SDN): research issues and challenges. *IEEE Commun Surv Tutor*. 2018; 21(1):393-430.

17. Braga R., Mota E., Passito A.. Lightweight DDoS flooding attack detection using NOX/OpenFlow. Paper presented at: Proceedings of the IEEE Local Computer Network Conference. Denver, CO, USA: IEEE; 2010:408-415.

18. Hu D, Hong P, Chen Y. FADM: DDoS flooding attack detection and mitigation system in software-defined networking. Paper presented at: Proceedings of the GLOBECOM 2017–2017 IEEE Global Communications Conference. IEEE: Singapore; 2017:1–7.

19. Chen Z, Jiang F, Cheng Y, Gu X, Liu W, Peng J. XGBoost classifier for DDoS attack detection and analysis in SDN-based cloud. Paper presented at: Proceedings of the 2018 IEEE International Conference on Big Data and Smart Computing (BIGCOMP). Shanghai, China: IEEE; 2018:251–256.

20. Dayal N., Srivastava S. Leveraging SDN for early detection and mitigation of DDoS attacks. Paper presented at: Proceedings of the International Conference on Communication Systems and Networks; 2018: 52–75; Springer, New York, NY.

21. Myint Oo M, Kamolphiwong S, Kamolphiwong T, Vasupongayya S. Advanced support vector machine-(ASVM-) based detection for distributed denial of service (DDoS) attack on software defined networking (sdn). *J Comput Netw Commun*. 2019; 2019:1–12.

22. Rahman O, Quraishi MAG, Lung CH. DDoS attacks detection and mitigation in SDN using machine learning. Paper presented at: Proceedings of the 2019 IEEE World Congress on Services (SERVICES). Milan, Italy: IEEE; Vol. 2642; 2019: 184–189.

23. Shakil M, Fuad Yousif Mohammed A, Arul R, Bashir AK, Choi JK. A novel dynamic framework to detect DDoS in SDN using metaheuristic clustering. *Trans Emerg Telecommun Technol*. 2019;33:e3622.

Shpur O. M., Havryliv T. M. HYBRID APPROACH TO ANOMALY DETECTION IN TELECOMMUNICATION IOT NETWORKS USING LIGHTWEIGHT ML MODELS

The article proposes a hybrid approach for effective detection and prevention of DDoS attacks, which, in the context of the rapidly growing number of IoT devices, enables anomaly detection without placing significant load on the devices and the network as a whole. The core of the approach is the development of an anomaly detection algorithm that allows a comprehensive evaluation and analysis of network traffic, using lightweight ML modules to ensure timely attack detection. The proposed approach uses a multi-layer model of the management system, which includes the access level, Edge analysis on AWS Greengrass servers, SDN, and cloud artificial intelligence, and allows traffic analysis to be performed closer to the source, minimizing delays and load on central servers. At the Edge level, the first stage of analysis is performed using lightweight machine learning methods, such as entropy analysis, heuristic analysis of SYN requests, and traffic classification using the Isolation Forest model. These methods effectively identify potential DDoS attacks, relying on statistical indicators such as traffic concentration, SYN request frequency, and changes in overall traffic volume. If at least one of the conditions is met – either a low entropy value from a single IP address, a high number of SYN requests, or spikes in them – the algorithm sends a notification to block the IP at the management level. An important stage is the integration with the SDN control level, where algorithms are used for real-time traffic management based on the obtained analysis results. The SDN controller can implement policies to block or limit traffic from the given IP address, allowing an immediate response to detected threats. The system automatically generates an alarm signal and applies protection policies when two out of three methods detect an anomaly. This significantly reduces response time to threats and ensures effective real-time protection. Additionally, at the cloud level, using Federated Learning and Reinforcement Learning technologies, the optimization of management policies and adaptation of the system to new types of attacks is carried out.

Key words: *DDoS attacks, anomaly detection, lightweight ML modules, IoT networks, AWS Greengrass, network traffic analysis.*