DOI 10.31891/2307-5732-2023-321-3-296-301
УДК 621.391 160164

НІЧЕПОРУК АНДРІЙ
Хмельницький національний університет
https://orcid.org/ 0000-0002-7230-9475
e-mail: andrey.nicheporuk@gmail.com
НІЧЕПОРУК АНАСТАСІЯ
Хмельницький національний університет
https://orcid.org/ 0000-0001-5366-5792
e-mail: eldess06@gmail.com
ДАНЧУК СЕРГІЙ
Хмельницький національний університет
https://orcid.org/0000-0001-7854-4556
e-mail: sergey.danchuk.p@gmail.com
КОРОТКОВ ЮРІЙ
Хмельницький національний університет
https://orcid.org/0000-0000-4544-4588
e-mail: qazswe707@gmail.com
ЦАВОЛИК ТАРАС
Західноукраїнський національний університет
https://orcid.org/0000-0002-1136-5705
e-mail: tth@wunu.edu.ua

# СИСТЕМА ЗБОРУ ДАНИХ ТА ВИЯВЛЕННЯ РОЗПОДІЛЕНИХ АТАК ВІДМОВА В ОБСЛУГОВУВАННІ У МЕРЕЖАХ НА ОСНОВІ ПРОТОКОЛУ RPL

*В роботі представлено систему збору даних та виявлення розподілених атак відмова в обслуговуванні у мережах на основі протоколу RPL. Система складається із трьох модулів: модуль збору даних, модуль класифікації та модуль виявлення. Головною особливістю модуля збору даних було те, що збір даних забезпечувався декількома сніферами, що встановлені у мережі, і з подальшою агрегацією зібраних даних. Для реалізації модуля класифікації проведено дослідження методу опорних векторів та багатошарового персептрона. Модуль виявлення використовувався для трансляції повідомлення про аномальну поведінку на решту вузлів IoT мережі, що містять ідентифікатор скопроментованого вузла та шлях до нього.*

*Ключові слова: розподілена атака відмова в обслуговуванні, сніфер, RPL мережа.*

NICHEPORUK ANDRII, NICHEPORUK ANASTASIIA, DANCHUK SERHII, KOROTKOV YURII
Khmelnytskyi National University
TSAVOLYK TARAS
West Ukrainian National University

## SYSTEM FOR DATA COLLECTION AND DETECTION OF DISTRIBUTED DENIAL OF SERVICE ATTACKS IN THE RPL-BASED NETWORKS

*Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks are among the main security threats to Internet of Things (IoT) networks today. This type of attack leads to the loss of access to the device or the resources it offers. Therefore, with the aim of countering such cyber threats, it is proposed, a system for data collection and detection of distributed denial of service in the RPL-based networks is presented. The system consists of three modules: a data gathering module, a classification module and a detection module. The main purpose of the data collection module is that data collection was provided by several sniffers installed in the RPL network and with subsequent aggregation of the collected data. For the implementation of the classification module, research was carried out on the method of support vector machines (SVM) and a multilayer perceptron (MLP). The detection module was used to broadcast a message about the abnormal behaviour to the rest of the RPL network nodes, containing the ID of the compromised node and the path to it.*

*To evaluate the efficiency of the proposed system that is based on the data collected by the data gathering module, a number of experiments are conducted. To obtain the data set for the experiments, an infrastructure based on the Ubuntu operating system and the Cooja simulator are deployed, which allowed to simulate the RPL network. Based on the operation of the deployed network, network traffic was collected that corresponded to both legitimate traffic and traffic during a black hole attack. The total number of test data was 24,023 samples. According to the research results, it is established that the SVM-based model demonstrated better performance level, in particular, the accuracy of detecting denial-of-service attacks was 89.6%, while the rate of false positives was 6%.*

*Keywords: distributed denial of service attack, sniffer, RPL network.*

## Вступ

Інтернет речей (IoT) об’єднує пристрої у комп’ютерну мережу й дозволяє їм збирати, аналізувати, обробляти та передавати дані іншим об’єктам (речам), що поєднані між собою через програмне забезпечення, програми або технічні пристрої. Проте гетерогенність середовища та безпровідний спосіб обміну даними робить мережі Інтернету речей потенційними цілями для зловмисників. Серед одних із основних загроз безпеці мережам IoT є атаки типу відмова в обслуговуванні (DoS) або розподілені атаки відмова в обслуговуванні (DDoS). Даний тип атак призводить до втрати доступу до пристрою або ресурсів, які він пропонує. Зловмисники реалізують велике коло різних способів атаки, але найпоширеніші з них полягають у бомбардуванні системи величезною кількістю непотрібних даних, щоб заповнити доступну пропускну здатність мережі цілі або її обчислювальну потужність [1]. Іншим варіантом впливу IoT мережу є

перенаправлення пакетів або їх відкидання [2]. Даний види атак особливо гостро проявляється у IoT мережах з огляду на характер реалізації алгоритмів маршрутизації, що передбачають використання повнозв'язних топологій та передачу даних від джерела до приймача через ланцюжок проміжних вузлів [3]. В загальному даний вид атак призводить до того, що легітимні користувачі втрачають доступ до ресурсів або пристроїв. Ще більше погіршує ситуацію для антивірусних засобів використання різних технік обфускації, які до прикладу використовуються у метаморфних вірусах [4–6]. Щодо мети реалізації таки атак, то вона може бути різна, починаючи від створення бот-мереж [7] для отримання грошової винагороди, і закінчуючи задоволенням власних амбіцій. На сьогоднішній день традиційні підходи виявлення атак відмова в обслуговуванні не відповідають поточним вимогам безпеки [8–10]. Існуючі методи та засоби не дозволяють у повному обсязі протистояти постійно зростаючим загрозам. Тому розробка нових методів виявлення атак відмова в обслуговуванні на інфраструктуру Інтернету речей є актуальним завданням.

**Архітектура системи збору даних та виявлення розподілених атак відмова в обслуговуванні у мережах на основі RPL протоколу**

Завдання збору даних у мережах Інтернету речей є одним напрямків процесу зворотної розробки та може бути імплементоване з метою виконання двох основних функцій: аналізу зібраних даних з метою підвищення ефективності взаємодії між пристроями в мережі або з метою здійснення діагностики мережі на предмет пошуку несправностей. В свою чергу одним із основних напрямків діагностики мереж є аналіз даних мережевого трафіку на предмет виявлення зловмисної активності або впливу кібератак. Це дозоляє реалізувати одну із головних вимог що ставиться до інфраструктури Інтернету речей – забезпечення її безпеки функціонування з точки зору здатності протидії впливу зловмисного програмного забезпечення та кібератак. В даній роботі представлено систему збору даних із протоколу маршрутизації RPL для виявлення розподілених атак відмова в обслуговуванні у мережах Інтернету речей, що функціонують на основі протоколів 6LoWPAN та RPL. Основу запропонованої системи складають три основних модулі (рис. 1): модуль збору даних (МЗД), модуль класифікації (МК), модуль виявлення (МВ).

Модуль збору даних (МЗД) можна розглядати як міжфазний модуль, оскільки він залучається у двох фазах функціонування системи: попереднього навчання та після навчання. Модуль виявлення та модуль агента вузла є частиною фази після навчання та відповідають за виявлення атак і формування реакції протидії. Крім того, на цьому етапі відбувається моніторинг трафіку, класифікація даних та ізоляція зловмисних вузлів. Узагальнену схему системи збору даних та виявлення розподілених атак відмова в обслуговуванні у мережах на основі RPL протоколу наведено на рис. 1.

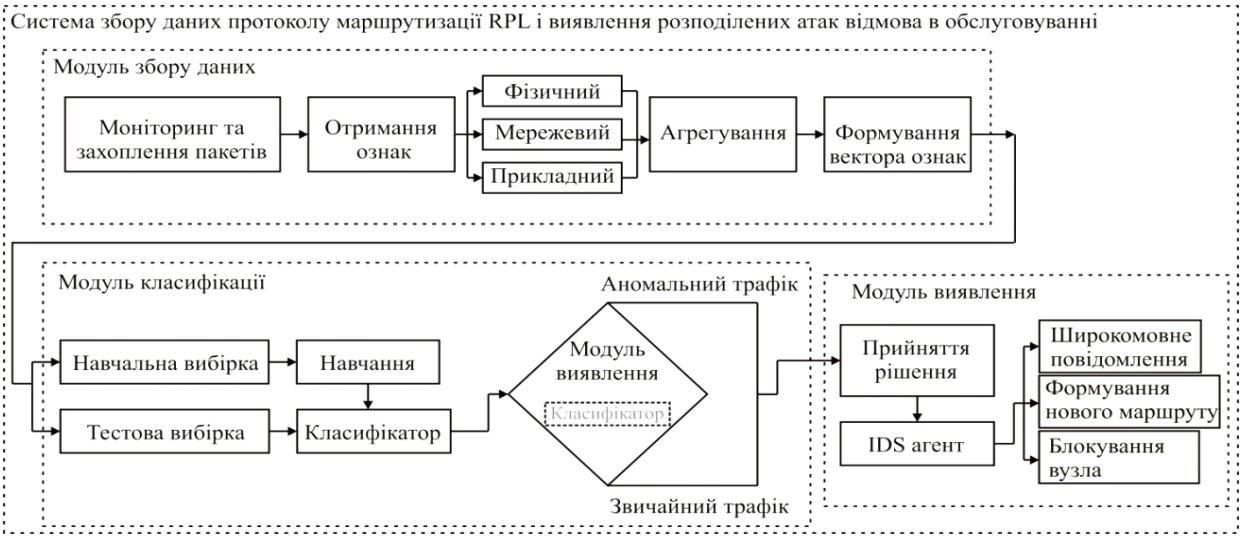


**Рис. 1. Архітектура системи збору даних та виявлення розподілених атак відмова в обслуговуванні у мережах на основі RPL протоколу**

**Модуль збору даних**

Перш ніж здійснити виявлення будь-якої зловмисної активності, слід отримати ознаки (features) із мережі, що дозволили б ідентифікувати появу аномалій. З цією метою у системі запропоновано модуль збору даних. Основною метою цього модуля є збір даних у реальній мережі Інтернету речей (або у модельованій мережі), що функціонує на основі протоколів 6LoWPAN і RPL. Слід відзначити, що запропонована архітектура системи збору даних і виявлення розподілених атак відмова в обслуговуванні не обмежується даними протоколами і у майбутньому може бути узагальнена та масштабована й для інших протоколів обміну даними в мережах Інтернету речей.

У даній системі пропонується використати ознаки із трьох логічних рівнів: фізичного, мережевого та прикладного рівнів. Опрацювання ознак фізичного рівня, зокрема таких як прийняті та передані dBm сигнали на рівні MAC, пов'язано із атаками глушіння фізичного рівня (jamming attacks), що переслідують мету порушення фізичного з'єднання між вузлами у мережі. В результаті опрацювання пакетів фізичного

рівня отримаємо ознаки показник рівня приймаючого сигналу RSSI ( $f^{p}_{RSSI}$ ), значення отриманого сигналу dBm ( $f^{p}_{RdBM}$ ), значення переданого сигналу dBm ( $f^{p}_{TdBM}$ ).

Отримання ознак мережевого рівня є важливим з огляду на специфіку функціонування багатьох відомих атак відмова в обслуговуванні (наприклад атаки вибіркового пересилання пакетів та black hole атака). Із пакетів цього рівня отримуються такі ознаки, як значення якості зв'язку ( $f^{n}_{LQI}$ ), середнє значення очікуваної кількості передач ETX ( $f^{n}_{ETX}$ ), кількість повідомлень DIO ( $f^{n}_{NDIO}$ ), кількість повідомлень DIS ( $f^{n}_{NDIS}$ ) та зміна рівня RPL (ранг) вузла ( $f^{n}_{LRPL}$ ).

На прикладному рівні даний модуль збирає специфічну для програми інформацію, таку як рівень потужності вузла та температура. Ознаки прикладного рівня, можна отримати шляхом програмування вузлів для розрахунку споживаної потужності електроенергії та інших пов'язаних функцій. Прикладний рівень є зв'язком між мережею та прикладним програмним забезпеченням. В даному дослідженні із пакетів прикладного рівня отримуються такі ознаки як середнє ( $f^{a}_{MeCP}$ ) та модальне значення споживаної потужності ( $f^{a}_{MoCP}$ ) та ідентифікатор вузла ( $f^{a}_{NID}$ ).

Процес вилучення ознак передбачає послідовне отримання ознак із кожного рівня та збереження їх до бази даних з метою їх подальшого опрацювання. Окремо слід відзначити, що перед вилученням ознак слід визначити часове вікно для агрегування даних у записи. Це часове вікно буде використано пізніше для отримання кількісних показників та середніх значень.

Таким чином в результаті опрацювання мережевого трафіку модулем збору даних буде отримано набір даних на основі протоколів RPL та LoWPAN, який буде використано для навчання та тестування алгоритму машинного навчання та створення моделі виявлення (фаза попереднього навчання). Також слід відзначити, що ідентичні кроки по відбору ознак проводяться і для фази після навчання, коли буде використана створена модель машинного навчання для аналізу невідомої активності в режимі реального часу.

**Модуль класифікації**

Набір даних, згенерований модулем збору даних, використовуватиметься для навчання та тестування алгоритмів машинного навчання. На цьому рівні виконується аналіз різних методів машинного навчання, а також здійснюється вибір того алгоритму, який має найкращі результати з точки зору ефективності та достовірності виявлення атак. В даній роботі в якості методів машинного навчання використаємо два найбільш поширенні методи для даної області дослідження, а саме метод опорних векторів та багатошаровий персептрон.

**Модуль виявлення**

Цей модуль працює як точка з'єднання між локальною мережею та системою виявлення розподілених атак відмова в обслуговувані на інфраструктуру Інтернету речей. Він побудований на вершині базової станції мережі (sink node), оскільки всі вузли підключені до базової станції або безпосередньо, або на відстані кількох переходів (hop). Основна функція цього модуля полягає в трансляції повідомлення про аномальну поведінку на решту вузлів IoT мережі, що містять ідентифікатор зловмисника та шлях до зловмисника. Це дозволить іншому незачепленому вузлу додати вузол зловмисника до чорного списку та уникнути будь-якого зв'язку зі зловмисним вузлом [11]. Крім того, агент виявлення змінює маршрут вузла-жертви та створює новий альтернативний шлях до вузла-приймача. Потім агент виявлення ініціює реконфігурацію топології мережі, щоб ізолювати зловмисний вузол шляхом встановлення нового маршруту до приймача від вузла-жертви. Усі вузли заносять у чорний список шкідливий вузол, а весь мережевий трафік від нього ігнорується та відкидається.

**Функціонування системи: фаза попереднього навчання та фаза після навчання**

Функціонування запропонованої системи збору даних протоколу маршрутизації RPL для виявлення розподілених атак відмова в обслуговуванні на інфраструктуру Інтернету речей включає дві фази: фазу попереднього навчання та фазу після навчання.

У фазі попереднього навчання модель машинного навчання навчається та тестується на основі зібраних даних МЗД. У даній роботі буде досліджено два алгоритми машинного навчання та проведено набір тестів для визначення найефективнішої моделі. Слід відзначити, що опрацювання моделей машинного навчання здійснюється на основі отриманих даних МЗД.

Процес вибору найкращого методу машинного навчання можна описати наступними кроками:

1. Вибір алгоритму: перед навчанням моделі необхідно вибрати тип машинного навчання. Загальну базу алгоритмів складають метод опорних векторів та штучна нейронна мережа. Слід відзначити, що даний набір може бути розширений, шляхом додавання інших алгоритмів машинного навчання.

2. Навчання/тестування: це фаза навчання для моделі машинного навчання, на якій дані передаються в обраний алгоритм для створення моделі машинного навчання.

3. Перевірка: на цьому етапі модель перевіряється за допомогою набору атрибутів і оцінок.

4. Оптимізація: на цьому кроці задана модель повторюється кілька ітерацій із іншим набором гіперпараметрів. Зазначені кроки повторюються допоки не буде отримано найоптимальніший модель для заданого алгоритму машинного навчання.

Наприкінці цих кроків генеруються дві оптимізовані моделі машинного навчання. На основі

результатів на етапі верифікації буде обрано найкращу модель, яка і буде розгорнута в інтелектуальній системі виявлення розподілених атак відмова в обслуговувані на інфраструктуру Інтернету речей.

Фаза після навчання відповідає за обробку даних і виконання активностей у режимі реальному часі. Роботу системи збору даних протоколу маршрутизації RPL для виявлення розподілених атак відмова в обслуговуванні у фазі після навчання подамо у вигляді наступної послідовності етапів:

1. Агрегація трафіку. Даний крок передбачає збір даних з декількох сніферів, що функціонують у мережі Інтернету речей. Підтримка кількох сніферів у мережі має важливе значення для забезпечення масштабованості мережі та покриття виявлення атак, особливо, якщо мова йде про розподілені атаки, що націлені на декілька вузлів.

З метою перевірки унікальності пакетів, здійснюється порівняння пакетів за часовою міткою. Далі якщо відбулось співпадіння, здійснюється перевірка по значенню ідентифікатора вузла. Таким чином сигнатура даних визначимо як пару значень <часова містка, ідентифікатор вузла>. Якщо підпис пакета дорівнює будь-яким пакетам, отриманим від будь-якого іншого сніфера, один із пакетів буде проігноровано, і лише одну версію пакета буде додано до черги. В іншому випадку додаткова процедура не потрібна, і пакети пересилаються до наступного набору. Цей процес забезпечує відсутність дублювання даних у режимі реальному часі. Слід відзначити, що процес отримання даних здійснюється на протязі часового вікна w. Таким чином, мережевий трафік розбивається на k інтервалів, довжиною w.

2. Вилучення ознак. Даний крок передбачає виконання тієї самої послідовності дії, що й для фази попереднього навчання (в режимі офлайн), за тим лиш виключенням, що цей процес виконується в режимі реального часу для мереж Інтернету речей.

3. Класифікація атак. На основі отриманої у фазі попереднього навчання оптимальної моделі машинного навчання здійснюється класифікація аномалій у мережевому трафіку.

4. Формування результатів. На цьому кроці здійснюється генерація результату виявлення та створення й надсилання UDP пакету агенту виявлення. Пакет містить такі параметри як ідентифікатор вузла, часова мітка, батьки вузла, ранг і результат виявлення. Результат виявлення є змінною, яка може приймати два значення – 0 або 1. Якщо результат дорівнює 0, то це вказує на те, що жодної атаки не виявлено, і подальші пакети не будуть надіслані агенту виявлення. В іншому випадку, якщо результат виявлення дорівнює 1, пакет із результатом виявлення надсилається агенту виявлення.

Окремо слід відзначити про аномальну поведінку у мережі при якій здійснюється активація фази після навчання. Загалом аномалією вважається зміна параметрів мережі у порівнянні із усталеними показниками цих показників більше ніж заданий поріг чутливості. Значення порогу чутливості є емпіричним числом, що специфічне для кожної мережі. У даній роботі показниками, що є тригерами для активації фази після навчання є:

Зміна кількості інформаційних повідомлень DIO. Заданий вузол у дереві DODAG може розсилати це повідомлення, яке дозволяє іншим вузлам дізнатись про нього. Це повідомлення використовується з метою отримати інформацію про те, чи є вузли, які хочуть приєднатись до дерева.

Зміна кількості інформаційних повідомлень DIS. Якщо відсутнє повідомлення DIO, і якщо вузол хоче приєднатися до дерева DODAG, він надсилає дане контрольне повідомлення. Таким чином DIS дозволяє згенерувати запит на пошук будь-яких DODAG.

**Отримання даних та перевірка достовірності виявлення розподілених атак відмова в обслуговуванні**

Для отримання набору даних для проведення експериментів було розгорнуто інфраструктуру на основі операційної системи Ubuntu та симулятора Cooja [12]. При моделюванні мережі на основі протоколу RPL усі давачі (звичайні вузли і вузли, що представляють базові станції) використано один і той самий тип мота – Zolertia Z1. Для отримання тестових даних розгорнуто гомогенну мережу, що складалась із двох типів вузлів – базової станції та клієнтських вузлів. Основне завдання, що вирішувалось у модельованій мережі було вимірювання температури. Це завдання виконувалось клієнтськими вузлами, що виконували вимірювання та надсилання базовій станції температури з інтервалом у 20 секунд. Разом із цими даними у пакетах UDP, що відправлялись на базову станцію, отримувалась інша службова інформація, така як рівень RSSI, LQI (індикатор якості зв'язку) та значення ETX. Базова станція представляла кореневий вузол, що виконував функцію не тільки організуючу (підтримує ієрархію зв'язків між вузами у мережі IoT), а й працював як сервер, на який надходили дані від клієнтських вузлів. Окрім того даний вузол був містком між IoT мережею та граничним маршрутизатором. Організація базової станції та її функціональність реалізована за допомогою компонентів у Contiki OS.

Усі вузли у модельованій мережі працюють під керуванням модифікованої операційної системи Contiki 3.0, включаючи вузли-сніфери. З точки зору маршрутизації було використано стандартний мережевий стек в Contiki OS на основі протоколу RPL. Граничний маршрутизатор реалізовано на основі операційної системи Ubuntu 22.04, яка обробляє всі з'єднання, що надходять від сніферів і базових станцій. Для реалізації сніферів було використано засіб WireShark. На рисунку 3 наведено результати процесу моделювання розгорнутої IoT мережі в Cooja.

В якості розподіленої атаки відмова в обслуговуванні, яка використовувалась для тестування запропонованої системи, було обрано атака скидання пакетів, у якій маршрутизатор, за принципом роботи повинен ретранслювати пакети, проте натомість відкидає їх. В даному дослідженні для реалізації атаки скидання пакетів було використано RPL Attacks Framework [13].

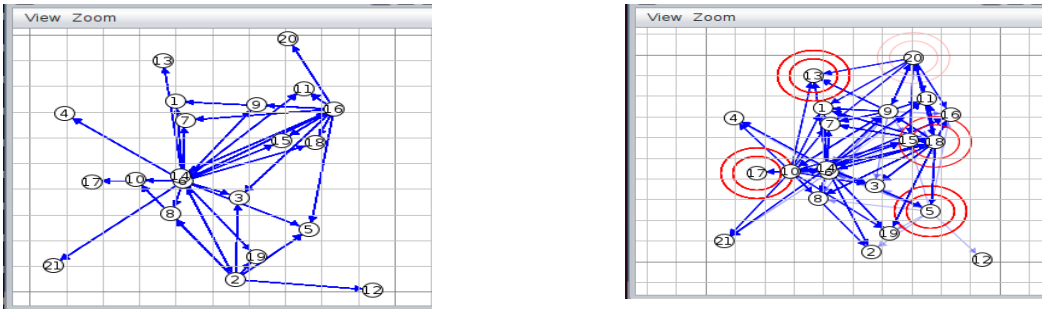


**Рис. 2. 6LoWPAN-RPL мережа для моделювання в Cooja**

В результаті моделювання бездротової сенсорної мережі було отримано 24 023 векторів ознак, що отримані із IEEE 802.15.4, 6LoWPAN, IPv6 та ICMPv6 пакетів. Із отриманих векторів ознак до класу malicious traffic віднесено 14596 зразків, а до класу legitimate traffic 9426 векторів ознак.

Для створення моделі виявлення у системі виявлення розподілених атак відмова в обслуговуванні весь набір даних був поділений на 2 частини: навчальна та тестова вибірка.

Навчальний набір даних це набір векторів ознак, які використовуються для процесу навчання та підгонки параметрів класифікатора. Даний набір складає 80% всіх векторів ознак із обох класів (тобто 7 540 зразків легітимного трафіку та 11 676 зразків, що промарковані як malicious traffic). Таким чином навчальний набір даних використовується для створення моделей, які є кандидатами для розпізнавання шкідливої активності у мережевому трафіку.

Для підбору оптимальних гіперпараметрів для кожної моделі було використано метод K-перехресної перевірки. Даний метод використовується для пошуку оптимальних гіперпараметрів моделі та нівелювання процесів недонавчання та перенавчання моделі.

Для виконання K-перехресної перевірки вся множина навчальної вибірки була поділена на дві частини: навчальну та вибірку для валідації. В якості K було вибрано значення 8. Це означає, що із 8 частин, навчання моделі проводиться на 7 частинах, а перевірка здійснюється на тій, що залишилась. Даний процес ітеративно продовжувався допоки кожна із 8 частин була використана як тестовий набір. На кожній ітерації проводилось оцінка моделі класифікатора із використанням міри F1. За результатами всі K навчань та перевірок класифікатора було визначено усереднене значення міри F1.

Для моделі штучної нейронної мережі було використано багатошаровий персептрон із зворотним розповсюдженням помилки. В якості гіперпараметрів для запропонованої ШНМ було досліджено кількість прихованих шарів, значення альфа та функцію активації. Кількість прихованих шарів використовується для визначення кількості шарів між входом мережі та виходом мережі та кількості нейронів у кожному прихованому шарі. Значення альфа використовується для регуляризації, та визначає штрафне значення, яке використовується для визначення розміру ваг, що використовуються для запобігання перенавчанню.

За результатами проведених експериментів по визначенню оптимальних параметрів оптимальне значення кількості прихованих шарів становить (6,4), функція активація ReLU, а значення альфа 0,001.

В якості гіперпараметрів для моделі на основі SVM обрано значення C та Гамма. Параметр C повідомляє у SVM визначає, наскільки потрібно уникнути неправильної класифікації кожного прикладу при навчанні. Для великих значень C оптимізація вибере гіперплощину з меншим запасом, якщо ця гіперплощина краще справляється з правильною класифікацією всіх навчальних точок. І навпаки, дуже мале значення C змусить оптимізатор шукати роздільну гіперплощину з більшим запасом, навіть якщо ця гіперплощина неправильно класифікує більше точок. Ядром SVM обрано радіальну базисну функцію, у якій параметр гама визначає вплив точки на кривизну рішення.

За результатами проведених експериментів оптимальними гіперпараметрами для SVM було визначено значення C на рівні 1 та параметром гамма, що складає 0,001. Як і для ШНМ визначення гіперпараметрів для SVM проводилось на основі K-перехресної перевірки.

Таблиця 1

**Оцінка достовірності роботи системи виявлення розподілених атак відмова в обслуговувані на інфраструктуру Інтернету речей для ШНМ та SVM**

| Модель класифікатора | Спостереження | | | | Метрика |
|---|---|---|---|---|---|
| | TP | FP | TN | FN | Accuracy |
| ШНМ | 2546 | 264 | 1622 | 374 | 0,867 |
| SVM | 2686 | 298 | 1588 | 234 | 0,896 |

Для визначення ефективності запропонованої системи, проведено експеримент, що полягав у оцінці процесу виявлення розподілених атак відмова в обслуговуванні двома моделями класифікаторами, що отримані на попередньому кроці. В якості метрик для оцінки було використано Accuracy:

В якості нульової гіпотези H0 було визначено твердження, яке можна сформулювати наступним чином: «зразок мережевого трафіку має ознаки аномальності та може бути атакою скидання пакетів».

За результатами проведених експериментів можна зробити висновок, що обидві моделі класифікаторів, що представляють ядро модуля виявлення у запропонованій системі, продемонстрували достовірність виявлення більшу за 85%. Кращим отриманні результати у моделі на основі SVM (достовірність виявлення 89,6%) із рівнем хибних позитивних спрацювань (помилок першого роду) 6% та рівнем хибно негативних спрацювань 4,87%. Слід відзначити, що модель на основі штучної нейронної мережі показала результати помилок першого роду на рівні 5,5, що є меншим відповідне значення у моделі SVM. Проте з точки зору критичності для кінцевих користувачів важливішим є помилки другого роду, які є в даному експерименті кращими саме у моделі на основі SVM.

**Висновки**

В результаті проведеного дослідження представлено систему збору даних із протоколу маршрутизації RPL для виявлення розподілених атак відмова в обслуговуванні у мережах Інтернету речей, що функціонують на основі протоколів 6LoWPAN та RPL. Основу запропонованої системи складають три основні модулі: модуль збору даних, модуль класифікації та модуль виявлення. Особливістю модуля збору даних було те, що збір даних забезпечувався декількома сніферами, що встановлені у мережі, і з подальшою агрегацією зібраних даних. В основі модуля класифікації було досліджено два алгоритми машинного навчання: метод опорних векторів та багатошаровий персептрон. Модуль виявлення використовувався для трансляції повідомлення про аномальну поведінку на решту вузлів IoT мережі, що містять ідентифікатор скопроментованого вузла та шлях до нього.

Метою проведення експериментів було оцінка достовірності виявлення розподілених атак відмова в обслуговуванні на наборі даних отриманому модулем збору даних. Для отримання набору даних для проведення експериментів було розгорнуто інфраструктуру на основі операційної системи Ubuntu та симулятора Cooja, що дозволило змоделювати RPL мережу, основним завданням вузлів якої було вимірювання температури та надсилання отриманого значення на базову станцію. Ґрунтуючись на функціонуванні розгорнутої мережі було зібрано мережевий трафік, що відповідав як легітимному трафіку так і трафіку при впливу атаки відмова в обслуговуванні. Загальна кількість тестових даних склала 24 023 зразків. В якості атаки для дослідження було задіяно атаку скидання пакетів. За результатами проведених експериментів модель на основі SVM показала кращі показники достовірності, із рівнем хибних позитивних спрацювань 6% та рівнем хибно негативних спрацювань 4,87%.

**References**

1. Serrano B., Fernando J., Song W. (2021). A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. Engineering Science and Technology, an International Journal. 31. DOI: 10.1016/j.jestch.2021.09.011.

2. Kafke J., Viana T. (2022). Call Me Maybe: Using Dynamic Protocol Switching to Mitigate Denial-of-Service Attacks on VoIP Systems. Network. 2(4). p. 545–567.

3. Al-Hadhrami Y., Hussain F. K. (2020). Real time dataset generation framework for intrusion detection systems in IoT. Future Generation Computer Systems. 108. p. 414–423.

4. Pomorova O., Savenko O., Lysenko S. (2016). Metamorphic Viruses Detection Technique based on the Modified Emulators. CEUR Workshop Proceedings. 1614. p. 375–383.

5. Savenko O., Lysenko S., Nicheporuk A. (2017). Metamorphic Viruses' Detection Technique Based on the Equivalent Functional Block Search. CEUR Workshop Proceedings. 1844. p. 555–569.

6. Savenko O., Nicheporuk A., Hurman I., Lysenko S. (2019). Dynamic signature-based malware detection technique based on API call tracing. CEUR Workshop Proceedings. 2393. p. 633–643.

7. Pomorova O., Savenko O., Lysenko S., Kryshchuk A., Nicheporuk A. (2014). A Technique for detection of bots which are using polymorphic code. Communications in Computer and Information Science. 431. p. 265–276.

8. Jing H., J. Wang, C.L. (2022). Chen Detection of DDoS Attack within Industrial IoT Devices Based on Clustering and Graph Structure Features. Security and Communication Networks. 1401683. DOI: 10.1155/2022/1401683

9. Hussain F., Abbas S. G., Husnain M., Fayyaz U. U., Shahzad F., Shah G. A. (2020). IoT DoS and DDoS Attack Detection using ResNet. Proceedings of 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, p. 1–6. DOI: 10.1109/INMIC50486.2020.9318216.

10. Hong L., Wehbi K., Alsalah T. H. (2022). Hybrid Feature Selection for Efficient Detection of DDoS Attacks in IoT. Proceedings of the 2022 6th International Conference on Deep Learning Technologies (ICDLT '22), Association for Computing Machinery, New York, NY, USA, p. 120–127. DOI: 10.1145/3556677.3556687

11. Al-hadhrami Y., Hussain F. K. (2019). A Machine Learning Architecture Towards Detecting Denial of Service Attack in IoT. Conference on Complex, Intelligent, and Software Intensive Systems, Springer, p. 417–429.

12. Osterlind F., Dunkels A., Eriksson J., Finne N., Voigt T. (2006). Cross-Level Sensor Network Simulation with COOJA. Proceedings. 2006 31st IEEE Conference on Local Computer Networks, Tampa, FL, USA, p. 641-648. DOI: 10.1109/LCN.2006.322172

13. RPL Attacks Framework. URL: https://github.com/dhondta/rpl-attacks