https://doi.org/10.31891/2219-9365-2022-72-4-5
УДК 004.056:004.852

Антоніна КАШТАЛЬЯН
Хмельницький національний університет
e-mail: antonina.kashtalian@gmail.com
Денис ЛЮБІНЕЦЬКИЙ
Хмельницький національний університет
e-mail: kiberplayer@gmail.com

РОЗПОДІЛЕНА САМООРГАНІЗОВАНА СИСТЕМА ПРОГНОЗУВАННЯ ЗЛОВМИСНОЇ АКТИВНОСТІ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

У роботі розроблено самоорганізовану систему прогнозування зловмисної активності в комп'ютерній мережі згідно алгоритмів роботи глибокого навчання. Крім того, було представлено нову самоорганізовану інкрементну нейронну мережу під назвою FG-SOINN написану мовою програмування Python. У SOINN видалення вузлів і ребер визначається двома параметрами, які потрібно оптимізувати для кожної наявної програми за допомогою перехресної перевірки або подібних підходів повторної вибірки. FG-SOINN усуває цей недолік, розглядаючи видалення вузлів і ребер як невід'ємну частину процесу навчання. Було сформульовано три концепції для формування «сміттєвого забуття»: час простою, надійність і корисність завдяки чому мережа видаляє вузли та ребра. Така мережа базується на концепті «навчання без вчителя» і може працювати із штучними та реальними даними і, навіть, за раптових або повторюваних відхилень.

Keywords: система виявлення вторгнень, аналіз трафіку, глибоке навчання, нейронні мережі, зловмисна активність, самоорганізована система.

Antonina KASHTALIAN, Denys LIUBINETSKYI
Khmelnytskyi National University

DISTRIBUTED SELF-ORGANIZED SYSTEM FOR PREDICTING MALICIOUS ACTIVITY IN COMPUTER NETWORKS

In this article, a self-organized computer network protection system based on deep learning algorithms was considered In addition, a new self-organizing incremental neural network called FG-SOINN written in the Python programming language was presented. In the SOINN, node and edge removal is defined by two parameters that need to be optimized for each existing program using cross-validation or similar resampling approaches. FG-SOINN overcomes this drawback by treating node and edge removal as an integral part of the learning process. Three concepts were formulated to form "garbage oblivion": idle time, reliability, and utility by which the network removes nodes and edges. Such a network is based on the concept of "learning without a teacher" and will work both with artificial and real data and even with sudden or repeated deviationst.

Keywords: intrusion detection system, traffic analysis, deep learning, neural networks, malicious activity, self-organized system.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

З безперервним зростанням загроз і атак, є досить складним завданням точно і своєчасно виявити зловмисну активність у комп'ютерних мережах. На сьогодні запропоновано багато принципів, методів, систем до виявлення мережевих вторгнень. Однак вони стикаються з критичними проблемами через постійне збільшення нових загроз, які поточні системи не розуміють.

Мережева активність означає взаємодію різних комп'ютерів для досягнення певних цілей. Зловмисна діяльність стає все більшою проблемою в Інтернеті. Спамери використовують скомпрометовані комп'ютери для надсилання шкідливих даних[1]. Знання комп'ютерні атаки може допомогти передбачити таку активність [2]. Незловмисна діяльність, також, викликає занепокоєння: засоби відстеження реклами та мережі доставки вмісту можуть взаємодіяти з багатьма комп'ютерами. Дослідження доброякісної активності допомагають встановити базову лінію [3] або охарактеризувати його зростання. На жаль, важко зрозуміти масштаби цих потенційних загроз через децентралізацію Інтернету, тому виявлення зловмисної активності в комп'ютерних мережах стає досить складним завданням. Крім того, через часті кібератаки, можна спостерігати тенденцію до того, що вони стають дедалі якіснішими та кваліфікованими. Нездатність запобігти або виявити такі вторгнення може мати серйозні наслідки для користувачів такої мережі. Для запобігання впливу зловмисної активності потрібна система, яка буде розпізнавати шаблони мережевого підключення, щоб класифікувати відомі та невідомі вторгнення, але також вимагає періодичного перенавчання, щоб підтримувати продуктивність на високому рівні.

Постановка проблеми вирішення задач прогнозування зловмисної активності

Зловмисні кібератаки створюють серйозні проблеми безпеки, які потребують нової, гнучкої та більш надійної системи виявлення вторгнень (IDS). IDS — це інструмент проактивного виявлення

вторгнень, який використовується для автоматичного виявлення та класифікації вторгнень, атак або порушень політик безпеки. Більшість методів виявлення зловмисних дій, запропонованих у літературі, є методами, заснованими на правилах (збіг сигнатур) і методами прогнозованого моделювання (виявлення аномалій) [4], [5]. Методи, засновані на правилах, зазвичай використовують відомі зловмисні дії як базову лінію для порівняння з новими поведінками, які, як відомо, вказують на порушення безпеки [4]. Зазвичай це досягається шляхом вбудовування евристик для пошуку відомих шаблонів (сигнатур) у мережі та/або даних аудиту. Однак розробити сценарії зловмисної діяльності, які охоплюють усі шаблони та/або невидимі шаблони (тобто атаки нульового дня), досить складно. Крім того, зловмисники можуть знати про евристики виявлення, які вже використовуються механізмом, і намагатися їх уникнути. Тому, потрібні більш надійні методи, які можуть адаптуватися протягом роботи задля попередження зловмисної активності.

Для забезпечення захисту мережі системи потрібно вирішити три важливі проблеми, що пов'язані з безпекою мережі.

1. Перша проблема пов’язана зі швидким збільшення обсягу мережевих даних. Це зростання пов’язано з використанням Інтернету речей (IoT) [6], хмарних сервісів та стрімкого зростання мережі пристроїв. Удосконалення методів аналізу даних включає підвищення швидкості та надійності процесу аналізу.
2. Друга проблема полягає в тому, що більш точне відстеження та інтерпретація значно підвищує якість висновків. Аналіз NIDS (Network Instruction Detection System) вимагає більш контекстно-специфічних спостережень, які підкреслюють більш абстрактні спостереження та спостереження вищого рівня. Усі зміни поведінки мають бути відстежуваними до окремого користувача, версії операційної системи або протоколів певних програм.
3. Третя загроза сучасних мереж — це різноманітність протоколів і масивна передача даних у сучасних мережах. В цьому випадку, існує надзвичайно високий рівень складності, коли намагаються відрізнити ненормальну поведінку від нормальної. Це збільшує ймовірність ненадійних і суперечливих даних та збільшує потенціал впливу вразливостей нульового дня.

Алгоритми інкрементного навчання дозволяють класифікатору з часом уточнювати та вдосконалювати свої можливості (оскільки він обробляє все більшу кількість вхідних даних) на відміну від автономного або пакетного алгоритму навчання, де передбачається, що класифікатор піддається впливу вхідних даних у пакеті. Динаміка мережевих даних значно змінюється з часом, і застосування статичних навчених моделей поступово погіршує продуктивність виявлення, роблячи алгоритми навчання з вчителем непридатними для IDS.

Системи виявлення вторгнень можна розділити на категорії залежно від використовуваного методу виявлення. Відповідно до досліджень в [6], методології виявлення класифікуються на дві категорії: на основі сигнатур і на основі аномалій. Методологія виявлення згідно сигнатур використовує шаблони, попередньо визначені відомими атаками, і поширюється як набір сигнатур. Потім сигнатури порівнюються з шаблонами, виявленими в мережевому трафіку, щоб виявити можливі атаки. Незважаючи на ефективність щодо відомих загроз, такий метод не може виявити або запобігти невідомим атакам і не може підтримувати й оновлювати сигнатури для відомих або нещодавно виявлених атак. Навпаки, виявлення на основі аномалій зазвичай встановлює базовий/нормальний рівень, використовуючи статистично значущий трафік.

Залежно від використовуваної техніки аналізу даних процес навчання/тестування може використовувати або класифікацію, або кластеризацію. Дослідження щодо вдосконалення методів класифікації систем виявлення вторгнень, здебільшого зосереджені на оцінці альтернативних рішень для основного аналізу, включаючи нейронні мережі [7] [8], нечітку логіку [8] [9], генетичні алгоритми [10] та опорні векторні машини [11]. У той же час методи кластеризації в основному використовують k-середні та алгоритми виявлення викидів [12], [13]. Що стосується впровадження, [14] продемонстрував ефективність використання TensorFlow для аналізу набору даних NSL-KDD і виявлення шкідливого трафіку з точністю 96%. Як було підкреслено попередніми дослідженнями [6], SOINN і поступове навчання дійсно є дуже ефективними методами для вирішення проблем виявлення зловмисної активності.

Під час еволюції IDS стало очевидним, що гібридний підхід дає кращі результати завдяки його здатності розрізняти типи та види мережевих атак, використовуючи спочатку статистичні підходи, щоб покращити формулювання та форматування вхідних даних, а потім застосувати їх до механізму на основі штучного інтелекту. Коли механізм виявлення визначає, чи є трафік частиною атаки, пакети можуть бути зареєстровані або скинуті та частково передані на пристрої-одержувачі.

Постановка задачі

Із збільшенням кількості та розмірів даних потрібні алгоритми навчання, щоб ефективно працювати з великою кількістю сигналів. Крім того, набагато складнішим завданням для навчання без вчителя є ефективне та стійке вивчення даних із розподілів, у яких існують дані з шумами. Основна складність полягає в тому, що алгоритми навчання не мають попередніх знань про розподіл даних у цілому. Таким чином, при надходженні перших кількох даних певного розподілу, кількість даних недостатня для представлення всього розподілу. Наразі алгоритми навчання не можуть визначити, чи є ці дані шумними чи

нормальними. Отже, для кожної ітерації існуючі методи (такі як самоорганізуюча карта (SOM) [15], нейронний газ (NG) [16] тощо) мають реагувати на нові дані та оновлювати вагові вектори відповідних нейронів, що зазвичай викликає критичне відхилення відображення топології в результаті. Інша проблема полягає в тому, що в більшості самоорганізованих нейронних мереж «зростаючого типу», таких як зростаючий нейронний газ (GNG) [17], число нейронів буде постійно збільшуватися внаслідок зростання стратегії їх визначення. Велика кількість нейронів збільшує обчислювальні витрати на пошук нейронів-переможців на кожній ітерації, що робить процедуру навчання неефективною. Тому, для вирішення таких задач потрібен алгоритм який буде уникати цих проблем, що в значній мірі покращить ефективність самоорганізованої системи.

Задача дослідження полягає у створенні розподіленої самоорганізованої системи прогнозування зловмисної активності, а саме систему виявлення вторгнень на основі штучного інтелекту та модифікованого модуля самоорганізованої інкрементної нейронної мережі. Такий модуль повинен використовувати структуру техніки «сміттєвого забуття» на основі концепцій часу простою, надійності та корисності.

Реалізація поставленої задачі дозволить визначити, спроектувати та реалізувати систему прогнозуання зловмисної активності шляхом використання нейронних мереж та методів SOIIN.

Архітектура самоорграніозованої системи прогнозування

Для правильного функціонування системи роботи, спрямованого на визначення зловмисної активності, потрібно визначити її архітектуру.

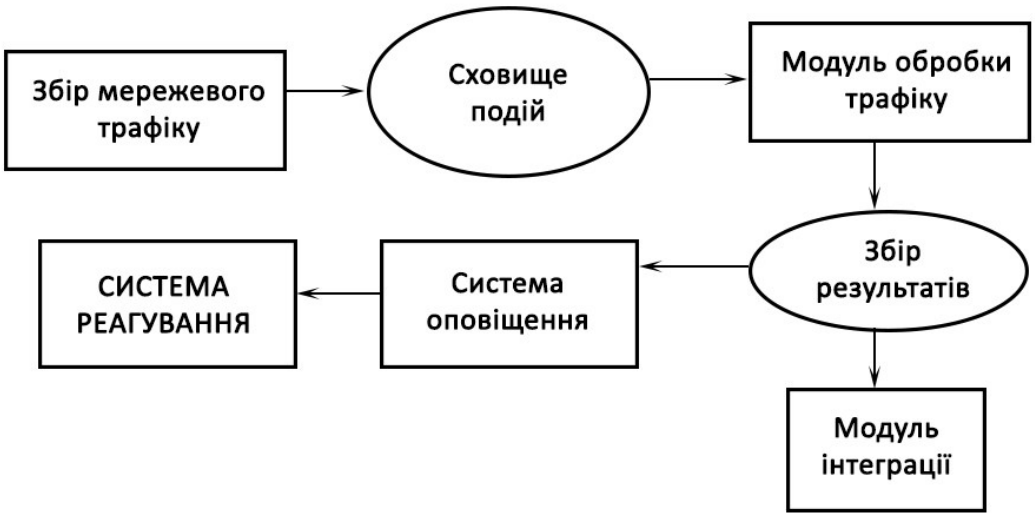

Рис. 1. Архітектура системи IDS на основі FG-SOINN

Така система буде складатися з наступних компонент:

Збір мережевого трафіку необхідний для збору всієї наявної інформації з пристроїв мережі. Крім того виконує функцію перетворення вихідного мережевого трафіку в необхідний вигляд (обрахування і визначеннння необхідних параметрів) і записування даних в сховище подій. Сховище вихідний подій визначене системою як місце для зберігання інформації, що надалі аналізується системою на наявність шкідливого трафіку і наявність мережевої атаки. Кожен запис у сховищі буде зберігати інформацію про потоки даних за параметрами, які необхідні для модуля обробки трафіку. Модуль обробки трафіку являє собою систему яка працює на алгоритмі самоорганізованих інкрементних нейронних мереж, розроблених у даній роботі. Він виконує аналіз трафіку кожного запису про потік, що зберігається в базі даних вихідних подій за допомогою алгоритмів, що використовують методи машинного навчання. В кінцевому результаті для кожного конкретного запису визначається тип з'єднання: нормальне або атака, а також вид самої атаки у випадку виявлення такої. Результати аналізу даних будуть занотовані в базу даних результатів. Місце збору результатів являє собою відокремлену базу даних, де зберігатимуться виявлені аномалії. Дана має використовуватися системою сповіщень, а також модулем сумісності для вилучення результатів аналізу. Система реагування буде виконувати функції «сміттяра». Кожен визначений системою шкідливий запис буде видалятися, не визначені записи, тобто ті записи, що не є і не нормальними і не шкідливими, буде повертатися у модуль обробки трафіку для подальшої повторної обробки. Надалі знову система звертається

до модуля збору мережевого трафіку для подальшого циклу роботи. Модуль інтеграції являє собою API для можливості інтегрування з системами реагування, інтерфейс системної взаємодії за допомогою http-запитів.

Основна частина

Самоорганізована інкрементна нейронна мережа (SOINN) — це механізм неконтрольованого навчання (або навчання без вчителя) для немаркованих даних. Самоорганізовані нейронні мережі відіграли важливу роль у сфері неконтрольованого навчання протягом останніх кількох десятиліть. Неконтрольоване навчання(навчання без вчителя) має дві основні цілі: кластеризацію та вивчення топології даних. Метою кластеризації є розділення даного набору даних на кілька кластерів, де кожна пара даних в одному кластері має більшу схожість, ніж у двох різних кластерах [18]. З іншого боку, навчання топології даних можна описати наступним чином: враховуючи розподіл даних високої розмірності, потрібно спроектувати вхідні дані в топологічну структуру, в якій дані у вхідному просторі проектуються топологічні суміжні одиниці [19]. Останнім часом ця техніка широко застосовується для інтелектуального аналізу даних, векторного квантування, розпізнавання образів, комп'ютерного зору та багатьох інших суміжних галузей [20].

Як неконтрольований інкрементний метод кластеризації, SOINN пропонує відносно високу швидкість обчислення з низькою обчислювальною вартістю. Крім того, складність мережі та розмір SOINN контролюються та стабілізуються за допомогою техніки «збирача сміття». Техніка визначає параметр виснаження, який називається віком, який представляє часові рамки, після яких вузли періоду буде видалено, якщо вони не оновлюються протягом зазначеного часу, і таким чином динамічно усуватиме шум у даних. Ця властивість робить його привабливим для динамічних середовищ, де потрібне тривале навчання. Щоб забезпечити її масштабованість під час розширення, розмір і зростання мережі контролюються параметром n, де кілька пар SOINN використовуватимуться як контрольований метод кластеризації. SOINN, як підсумовано на рисунку 1, ініціалізує мережу порожнім набором вузлів, потім додає перші два вузли до списку, використовуючи вагові вектори як два вхідних вектора [21]. Після ініціалізації нейронна мережа знаходить для кожного вхідного вектора найближчий вузол (переможець) і другий найближчий вузол (другий переможець) вхідного вектора, вимірюючи відстань S1 і S2 від кожного входу до кожного вузла за допомогою рівнянь (1) і (2). Дана формула є загальною формулою для вимірювання відстані між шарами.

$$s_1 = argmin_{C \in A} dist(x, w_c) \tag{1}$$

$$s_2 = argmin_{C \in A - \{s_1\}} dist(x, w_c) \tag{2}$$

Якщо вхідний вектор належить до того ж кластеру, що й переможець або другий переможець на основі відстаней, обчислених за пороговим критерієм подібності, SOINN оновлює ваговий вектор вузла та його сусідів із ваговим вектором вхідного значення та з'єднує його з вузол ребром. Якщо вхідний вектор не належить до того самого кластера переможця або другого переможця, механізм додає новий вузол до мережі.

Самоорганізуючі інкрементні нейронні мережі (SOINN) охоплюють сімейство нейронних мереж, спільним для яких є те, що вони знаходять топологічне відображення вхідних даних у мережеву структуру шляхом конкурентного навчання (21).

Можна сказати, що SOINN відображає p -вимірний вхід $x = x_1 x_2 \dots x_p$ де $x_i \in i^{-M}$ значенням ознаки для окремого вузла в неорієнтованому графі. Відображення відповідає точці в p - вимірному просторі ознак. Навчання в SOINN означає адаптацію топологічної карти: вузли можуть переміщатися, об'єднуватися з іншими вузлами, залишатися одиночними або видалятися, а межі між вузлами можна створювати або видаляти. Вузол треба розглядати як мікрокластер вхідних випадків, які знаходяться близько один до одного. Ребра можна розглядати як консолідовані зв'язки між пов'язаними вузлами, наприклад, вузлами, що належать одному (макро)кластеру.

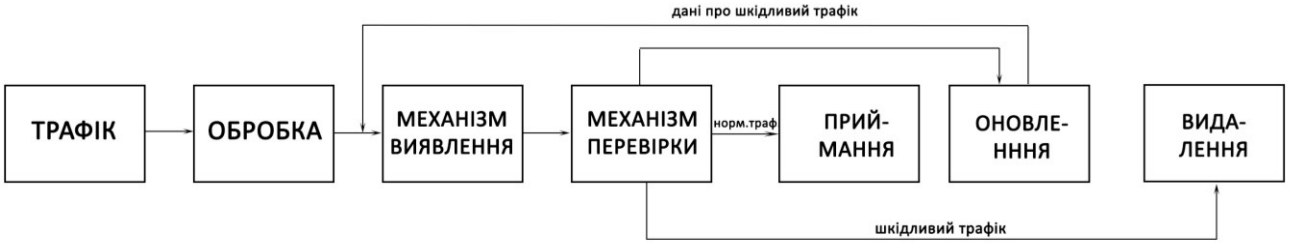

Рис. 2. Інформаційні потоки системи на основі FG-SOINN

На рисунку 2 зображено інформаційні потоки тієї частини системи, в якій досліджується трафік на предмет його класифікації. Спершу вхідний трафік зібраний системою подається на модуль попередньої

обробки. Цей модуль фіксує та обробляє вхідний трафік у реальному часі. Перехоплені TCP-з'єднання обробляються для вилучення відповідних функцій, які стають доступними як вхідний вектор для механізму виявлення – FG-SOINN. Для дослідження перевірка була виконана з використанням назви 41-го атрибуту набору даних NSL-KDD, і вся інформація про атрибути доступна в [22]. Структура базується на передумові, що характеристики TCP з'єднання вказують на те, чи з'єднання визначається як атака чи ні, і навіть якщо воно визначається як атака, то яким типом є ця атака. Далі інформація подається на механізм виявлення зловмисної активності, який після обробки передає інформацію про трафік на модуль механізму перевірки даних. Далі модуль перевірки визначає покращення та підвищення точності системи шляхом підтвердження передбаченої мітки. Саме на цьому етапі відбувається розподілення трафіку на шкідливий та нормальний. Після підтвердження того, що трафік є нормальним його передають користувачу для подальшої роботи. Але якщо система підтвердила виявлення шкідливого трафіку, модуль перевірки даних пересилає невдалі прогнози до модуля оновлення і видаляє з набору даних трафіку.

Модуль оновлення системи працює у дві фази: активна фаза та фаза оновлення. На фазі реального часу він приймає рішення на основі того, які його можливості були в той час, і на фазі оновлення, коли модуль оновлення оновлює систему за допомогою невдалих прогнозів, щоб покращити її можливості. Фази можуть виконуватися паралельно, якщо це необхідно у виробництві, або чергуватися відповідно до мережевого трафіку.

Основна концепція запропонованого алгоритму полягає в поступовому створенні механізму захисту мережі. На початковому етапі механізм виявлення навчається, використовуючи відносно невелику вибірку мережевих даних, достатню для базового захисту мережі. Згодом, коли стає доступним більше мережевих даних, механізм поступово оновлюється вхідними даними класів, які йому не вдалося виявити, щоб удосконалити та розширити свої захисні можливості. Щоб підтримати процес навчання, механізм перевірки вирішує, чи не вдалося прийняти рішення. Щоб розширити свої можливості, основний механізм виявлення повинен бути в змозі класифікувати мережеві дані за багатьма класами, не тільки про те, чи є з'єднання атакою чи ні, але й про тип атаки, а отже, пропонувати рішення для багатокласової проблеми поступового навчання.

Структура системи, використовує концепцію, що лежить в основі n-SOINN [23], яка модифікувала оригінальний SOINN для використання кількох пар SOINN з використанням підходу контрольованої кластеризації. n-SOINN використовує дві важливі модифікації: глобальний параметр, який контролює топологію мережі та використовує квадрат (а не базову) евклідову відстань для обчислення відстані між входом і вузлами [24]. Щоб контролювати кількість вихідних вузлів мережі, де різниця в тому, наскільки точно буде створена стиснена інформація, вводиться параметр з іменем n. Цей параметр диктує, що будь-який перший вузол-переможець, який виграє більше n разів, призначає перемогу другому вузлу-переможцю. Якщо другий вузол-переможець також має більше ніж n разів виграшу, генерується новий вузол. Для n=0 мережа поводиться точно так само, як вихідний SOINN. Встановлення дуже високих значень n зменшує кількість створених стабільних вузлів і надає перевагу лише популярним, що швидше за все, призведе до невеликої точності. Евклідова відстань, використана в оригінальному SOINN, була призначена для цілей єдиного SOINN для реалізації завдання інкрементного навчання без контролю (без вчителя). Використання квадрата евклідової відстані в n-SOINN дозволяє вимірювати відстань між вузлами для різних SOINN; старіння, вбудоване в забувач сміття (forgetting garbage або FG) SOINN дозволяє усувати вузли вхідних даних, коли вони стають непотрібними або не популярнимим. Основний модуль системи складається з двох основних частин: кластеризації та класифікатора. Блок кластеризації містить пару n-SOINN, які використовуються для кожного класу для стиснення інформації, отриманої від TCP-з'єднань модулем попередньої обробки, і досягнення інкрементного навчання. Частина класифікації приймає вихідні дані вузлів n-SOINNs, створює вхідні дані для класифікатора SVM для кожного класу виконання попередньої класифікації. Згодом m найвищих класів пар класифікації кожного класифікатора, відсортованих за оцінкою, потім класифікуються багатокласовою SVM для кінцевого рішення (m визначається користувачем відповідно до доступних класів). Оцінка базується на відстані зразків до розділової гіперплощини.

Експериментальне дослідження

Оцінка отриманої структури була виконана на наборі даних NSL-KDD [25], який є вдосконаленою версією відомого набору даних KDD'99. Незважаючи на свій вік, набір даних все ще є де-факто альтернативою для методів і інструментів порівняльного аналізу, які спрямовані на забезпечення ефективних систем виявлення вторгнень [26]. З огляду на його широке використання, що полегшує надання довідкового аналізу, було прийнято цей набір даних для початкового тестування впровадженого методу. Для негативного SOINN було використано n=2, а для позитивного SOINN n=100. Оскільки набір даних включав суміш звичайного трафіку та чотирьох атак, для цього експерименту було створено п'ять бінарних класів – звичайний клас і чотири класи атак (відмова в обслуговуванні, зондування, R2L і U2R).

Використаний набір даних включав дві різні підмножини, одну з 125973 записами, а іншу з 22544 записами (рис.4).

```
rand_int = random.randint(1, len(train) - 1)
x1 = train.iloc[rand_int].values
rand_int = random.randint(1, len(train) - 1)
x2 = train.iloc[rand_int].values
rand_int = random.randint(1, len(train) - 1)
x3 = train.iloc[rand_int].values

s = SF_SOINN(x1, x2, x3, max_edge_age=100, iter_lambda=100)

xs, n_nodes, n_edges, n_del_nodes, n_del_edges = train_phase(mode

Час навчання: 21 хв 29 сек
Вхідні дані оброблено: 125972
Кількість вузлів: 1076
Кількість ребер: 4712
```

Рис. 4. Обробка даних NSL-KDD

Друга підмножина не з того ж розподілу ймовірностей, що й перша, і також містить певні типи атак, яких немає в першій. Для базової оцінки та для того, щоб показати, що досягається поступове навчання, ми розділили першу підмножину на п’ять менших підмножин, які використовуються для раундів тестування/оновлення, і використали другу підмножину з 22543 записами для початкового навчання. Слід зазначити, що після початкового навчання для кожного раунду оновлення підмножина перевіряється на навченій FG-SOINN, і лише невдалі прогнози повертаються в систему.

```
Час  для фази оновлення: 7 хв 39 сек
Значень в обробці: 22543
Точність (відсоток правильно передбачених випадків): 93.44%
Відсоток виявлення (TPR): 93.77%
Хибнопозитивний рівень (FPR - нормально класифікується як напади): 6.99%
Рівень помилкових негативних результатів (FNR - напади класифікуються як нормальні): 6.23%
Можливість виявлення вторгнень (CID): 64.81%

{'warezmaster-normal': 161, 'saint-satan': 123, 'satan-saint': 120, 'back-normal': 117, 'normal-warezmaster': 104, 'normal-mai

update_phase(model=s, data=test_n21, labels=y_test_n21)

Час  для фази оновлення: 4 хв 0 сек
Значень в обробці: 11849
Точність (відсоток правильно передбачених випадків): 94.54%
Відсоток виявлення (TPR): 94.43%
Хибнопозитивний рівень (FPR - нормально класифікується як напади): 2.49%
Рівень помилкових негативних результатів (FNR - напади класифікуються як нормальні): 2.57%
Можливість виявлення вторгнень (CID): 71.7%

{'warezmaster-normal': 143, 'processtable-guess_passwd': 118, 'satan-saint': 114, 'guess_passwd-processtable': 111, 'saint-sat

update_phase(model=s, data=test_21, labels=y_test_21)

Час  для фази оновлення: 3 хв 31 сек
Значень в обробці: 10693
Точність (відсоток правильно передбачених випадків): 99.42%
Відсоток виявлення (TPR): 99.87%
Хибнопозитивний рівень (FPR - нормально класифікується як напади): 0.77%
Рівень помилкових негативних результатів (FNR - напади класифікуються як нормальні): 0.13%
Можливість виявлення вторгнень (CID): 94.99%
```

Рис. 5. Результати тренування системи після трьох раундів

Таблиця 1

Результати тренування FG-SOINN

Фаза оновлення	Точність [%]	Час [s]	Зразки
1	93.44	459	22543
2	94.54	699	37392
3	99.42	910	48085

Результати показані на рисунку 5, вказують на те, що структура може використовувати поступове навчання для досягнення суттєвих покращень. Така система визначає 5 основних показників:

- точність або відсоток виявлення випадків;
- справжній позитивний коефіцієнт (TPR) або коефіцієнт виявлення (DR): співвідношення між кількістю правильно передбачених атак і загальною кількістю атак, також називається коефіцієнтом виявлення (DR);
- рівень хибнопозитивних результатів (FPR): співвідношення між кількістю звичайних випадків, неправильно класифікованих як атаки, та загальною кількістю звичайних випадків;
- хибнонегативний показник (FNR): не вдалося визначити аномалію та класифікувати як нормальний;
- можливість виявлення вторгнень (CID): співвідношення спільної інформації між входом і виходом та ентропією входу.

Дані показники визначаються як метрики оцінки алгоритму роботи. Зразки, наведені в таблиці 1 є накопиченими зразками з попереднього раунду. Наприклад, для початкового навчання використовувався набір даних, що містив 22543 записи, а для першого раунду оновлень було використано 11849 записи, тобто кількість невдалих прогнозів для першої підмножини з п'яти накопичується до 37392. Точність навчання покращується з кожною новою фазою, що підтверджує твердження про ефективність запропонованої структури.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

В роботі запропонована самоорганізована система прогнозування зловмисної активності на основі інкрементного навчання. Виконується вона з допомогою системи виявлення вторгнень яка навчається з допомогою нейронних мереж. Запропонована структура та результати вказують на те, що така пропозиція може адаптуватися до природи динамічного профілю мережевих даних як для звичайних категорій, так і для категорій атак. Система використовує менше ресурсів, є швидшою і має вищу швидкість виявлення, ніж методи навчання з вчителем. Забезпечуючи систему невдалими прогнозами, ми не лише досягаємо поступового навчання з багатообіцяючою точністю, але й ефективну структуру, тобто замість того, щоб подавати їй повний набір даних, FG-SOINN зберігає лише частину набору даних, роблячи дану структуру дуже хорошим кандидатом для систем масштабування. Незважаючи на те, що час навчання системи збільшується зі збільшенням вхідних даних оновлення, режими оновлення системи та робочий режим можуть або працювати паралельно (одночасно), або режим оновлення може перемикатися, коли робоча фаза неактивна (тобто немає вхідних даних для виявлення). Таким чином вона набуває здібностей шляхом вивчення нових вхідних даних або невдалих класифікацій. Саме через ці здібності система буде вважатися самоорганізованою.

Програма була реалізована з допомогою середовища Jupiter Notebook та мови програмування Python. Така система здатна прогнозувати зловмисну активність та одночасно навчатися на невдалих попередніх спробах, що робить її більш ефективною перед штучними та реальними даними.

Література

1. Huang D. Y. et al. Tracking ransomware end-to-end //2018 IEEE Symposium on Security and Privacy (SP). – IEEE, 2018. – С. 618-631.

2. J. Czyz et al., "Taming the 800 pound gorilla: The rise and decline of NTP DDoS attacks," in Proc. ACM Internet Meas. Conf., Vancouver,BC, Canada, Nov. 2014, pp. 435–448.

3. E. Wustrow, M. Karir, M. Bailey, F. Jahanian, and G. Houston, "Internetbackground radiation revisited," in Proc. 10th ACM Internet Meas. Conf. ,Melbourne, VIC, Australia, Nov. 2014, pp. 62–74

4. Chattopadhyay M. Modelling of intrusion detection system using artificial intelligence—evaluation of performance measures //Complex System Modelling and Control Through Intelligent Soft Computations. – Springer, Cham, 2015. – С. 311-336.

5. Constantinides C. et al. A novel online incremental learning intrusion prevention system //2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). – IEEE, 2019. – С. 1-6.

6. Gokhale P., Bhat O., Bhat S. Introduction to IOT //International Advanced Research Journal in Science, Engineering and Technology. – 2018. – Т. 5. – №. 1. – С. 41-44.

7. Santikellur P. et al. Optimized multi-layer hierarchical network intrusion detection system with genetic algorithms //2019 2nd International Conference on new Trends in Computing Sciences (ICTCS). – IEEE, 2019. – С. 1-7.

8. J. J. Stephan, S. Mohammed, and M. K. Abbas, “Neural Network Approach to Web Application Protection,” Int. J. Inf. Educ. Technol., vol. 5, no. 4, 2015.

9. S. N. Shiaeles, V. Katos, A. S. Karakos, and B. K. Papadopoulos, “Real time DDoS detection using fuzzy estimators,” Comput. Secur., vol. 31, no. 6, pp. 782–790, 2012

10. Varzaneh Z. A., Kuchaki Rafsanjani M. Intrusion detection system using a new fuzzy rule-based classification system based on genetic algorithm //Intelligent Decision Technologies. – 2021. – Т. 15. – №. 2. – С. 231-237.

11. Y. Li, J. Xia, S. Zhang, J. Yan, X. Ai, and K. Dai, “An efficient intrusion detection system based on support vector machines and gradually feature removal method,” Expert Syst. Appl., vol. 39, no. 1, pp. 424–430, 2012.

12. M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, “A multi-step outlier-based anomaly detection approach to network-wide traffic,” Inf. Sci. (Ny)., vol. 348, pp. 243–271, 2016

13. T. Bakhshi and B. Ghita, “User traffic profiling,” in 2015 Internet Technologies and Applications (ITA), 2015, pp. 91–97.

14. L.-D. Chou et al., “Classification of Malicious Traffic Using TensorFlow Machine Learning,” in International Conference on Information and Communication Technology Convergence, 2018, pp. 186–190.

15. Zhang J. et al. Intelligent fault diagnosis of rolling bearings using variational mode decomposition and self-organizing feature map //Journal of Vibration and Control. – 2020. – Т. 26. – №. 21-22. – С. 1886-1897.

16. E. J. Palomo and E. López-Rubio, "The Growing Hierarchical Neural Gas Self-Organizing Neural Network," in IEEE Transactions on Neural Networks and Learning Systems, vol. 28, no. 9, pp. 2000-2009, Sept. 2017, doi: 10.1109/TNNLS.2016.2570124.

17. H.-J. Liao, C.-H. Richard Lin, Y.-C. Lin, and K.-Y.Tung, “Intrusion detection system: A comprehensive review,” J. Netw. Comput. Appl., vol. 36, no. 1, pp. 16–24, 2013.

18. R. Xu and D. C. W. II, “Survey of clustering algorithms.” IEEE Trans. Neural Netw., vol. 16, № 3, pp. 645–678, 2015

19. T. Martinetz and K. Schulten, “Topology representing networks,” Neural Networks, vol. 7, no. 3, pp. 507–522, 2014

20. K.-L. Du, “Clustering: A neural network approach,” Neural Networks, vol. 23, no. 1, pp. 89–107, 2010.

21. Furao S., Ogura T., Hasegawa O. An enhanced self-organizing incremental neural network for online unsupervised learning //Neural Networks. – 2007. – Т. 20. – №. 8. – С. 893-903.

22. Meena G., Choudhary R. R. A review paper on IDS classification using KDD 99 and NSL KDD dataset in WEKA //2017 International Conference on Computer, Communications and Electronics (Comptelix). – IEEE, 2017. – С. 553-558.

23. P. Kankuekul, A. Kawewong, S. Tangruamsub, and O. Hasegawa, “Online incremental attribute-based zero-shot learning,” 2012 IEEE Conference on Computer Vision and Pattern Recognition. IEEE, 2012.

24. S. Furao and O. Hasegawa, “An incremental network for on-line unsupervised classification and topology learning,” Neural Networks, vol. 19, no. 1, pp. 90–106, 20016.

25. Cervantes J. et al. A comprehensive survey on support vector machine classification: Applications, challenges and trends //Neurocomputing. – 2020. – Т. 408. – С. 189-215.

26. L. Dhanabal and D. S. P. Shantharajah, “A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms,” 2015.

References

1. Huang D. Y. et al. Tracking ransomware end-to-end //2018 IEEE Symposium on Security and Privacy (SP). – IEEE, 2018. – С. 618-631.

2. J. Czyz et al., “Taming the 800 pound gorilla: The rise and decline of NTP DDoS attacks,” in Proc. ACM Internet Meas. Conf., Vancouver,BC, Canada, Nov. 2014, pp. 435–448.

3. E. Wustrow, M. Karir, M. Bailey, F. Jahanian, and G. Houston, “Internetbackground radiation revisited,” in Proc. 10th ACM Internet Meas. Conf. ,Melbourne, VIC, Australia, Nov. 2014, pp. 62–74

4. Chattopadhyay M. Modelling of intrusion detection system using artificial intelligence—evaluation of performance measures //Complex System Modelling and Control Through Intelligent Soft Computations. – Springer, Cham, 2015. – С. 311-336.

5. Constantinides C. et al. A novel online incremental learning intrusion prevention system //2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). – IEEE, 2019. – С. 1-6.

6. Gokhale P., Bhat O., Bhat S. Introduction to IOT //International Advanced Research Journal in Science, Engineering and Technology. – 2018. – Т. 5. – №. 1. – С. 41-44.

7. Santikellur P. et al. Optimized multi-layer hierarchical network intrusion detection system with genetic algorithms //2019 2nd International Conference on new Trends in Computing Sciences (ICTCS). – IEEE, 2019. – С. 1-7.

8. J. J. Stephan, S. Mohammed, and M. K. Abbas, “Neural Network Approach to Web Application Protection,” Int. J. Inf. Educ. Technol., vol. 5, no. 4, 2015.

9. S. N. Shiaeles, V. Katos, A. S. Karakos, and B. K. Papadopoulos, “Real time DDoS detection using fuzzy estimators,” Comput. Secur., vol. 31, no. 6, pp. 782–790, 2012

10. Varzaneh Z. A., Kuchaki Rafsanjani M. Intrusion detection system using a new fuzzy rule-based classification system based on genetic algorithm //Intelligent Decision Technologies. – 2021. – Т. 15. – №. 2. – С. 231-237.

11. Y. Li, J. Xia, S. Zhang, J. Yan, X. Ai, and K. Dai, “An efficient intrusion detection system based on support vector machines and gradually feature removal method,” Expert Syst. Appl., vol. 39, no. 1, pp. 424–430, 2012.

12. M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, “A multi-step outlier-based anomaly detection approach to network-wide traffic,” Inf. Sci. (Ny)., vol. 348, pp. 243–271, 2016

13. T. Bakhshi and B. Ghita, “User traffic profiling,” in 2015 Internet Technologies and Applications (ITA), 2015, pp. 91–97.

14. L.-D. Chou et al., “Classification of Malicious Traffic Using TensorFlow Machine Learning,” in International Conference on Information and Communication Technology Convergence, 2018, pp. 186–190.

15. Zhang J. et al. Intelligent fault diagnosis of rolling bearings using variational mode decomposition and self-organizing feature map //Journal of Vibration and Control. – 2020. – Т. 26. – №. 21-22. – С. 1886-1897.

16. E. J. Palomo and E. López-Rubio, "The Growing Hierarchical Neural Gas Self-Organizing Neural Network," in IEEE Transactions on Neural Networks and Learning Systems, vol. 28, no. 9, pp. 2000-2009, Sept. 2017, doi: 10.1109/TNNLS.2016.2570124.

17. H.-J. Liao, C.-H. Richard Lin, Y.-C. Lin, and K.-Y.Tung, “Intrusion detection system: A comprehensive review,” J. Netw. Comput. Appl., vol. 36, no. 1, pp. 16–24, 2013.

18. R. Xu and D. C. W. II, “Survey of clustering algorithms.” IEEE Trans. Neural Netw., vol. 16, № 3, pp. 645–678, 2015

19. T. Martinetz and K. Schulten, “Topology representing networks,” Neural Networks, vol. 7, no. 3, pp. 507–522, 2014

20. K.-L. Du, “Clustering: A neural network approach,” Neural Networks, vol. 23, no. 1, pp. 89–107, 2010.

21. Furao S., Ogura T., Hasegawa O. An enhanced self-organizing incremental neural network for online unsupervised learning //Neural Networks. – 2007. – Т. 20. – №. 8. – С. 893-903.

22. Meena G., Choudhary R. R. A review paper on IDS classification using KDD 99 and NSL KDD dataset in WEKA //2017 International Conference on Computer, Communications and Electronics (Comptelix). – IEEE, 2017. – С. 553-558.

23. P. Kankuekul, A. Kawewong, S. Tangruamsub, and O. Hasegawa, “Online incremental attribute-based zero-shot learning,” 2012 IEEE Conference on Computer Vision and Pattern Recognition. IEEE, 2012.

24. S. Furao and O. Hasegawa, “An incremental network for on-line unsupervised classification and topology learning,” Neural Networks, vol. 19, no. 1, pp. 90–106, 20016.

25. Cervantes J. et al. A comprehensive survey on support vector machine classification: Applications, challenges and trends //Neurocomputing. – 2020. – Т. 408. – С. 189-215.

26. L. Dhanabal and D. S. P. Shantharajah, “A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms,” 2015.