https://doi.org/10.31891/2219-9365-2024-78-46
УДК 004.056

ЛУЖЕЦЬКИЙ Володимир
Вінницький національний технічний університет
https://orcid.org/0000-0001-7466-7738
lva.kzi2002@gmail.com
САВИЦЬКА Людмила
Вінницький національний технічний університет
https://orcid.org/0000-0003-1130-2621
e-mail: savytska.liudmyla@vntu.edu.ua

АНАЛІЗ ПІДХОДІВ ЩОДО ВИЯВЛЕННЯ АНОМАЛІЙ В ДЕЦЕНТРАЛІЗОВАНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

У статті розглянуто сучасні підходи до виявлення аномалій у децентралізованих однорангових (пірингових) мережах. Особливу увагу приділено викликам, пов'язаним із децентралізованою архітектурою, відсутністю централізованого управління та збереженням приватності користувачів. Проаналізовано методи моніторингу мережевої активності, зокрема, методи на основі правил, статистичні моделі, алгоритми машинного навчання, теорії графів та блокчейну. Переваги та недоліки кожного підходу розглянуто у контексті різних загроз, таких як DoS-атаки, бот-мережі та розповсюдження шкідливого ПЗ. Наведено приклади практичних реалізацій, зокрема систему GNUnet, їхні сильні та слабкі сторони. Підкреслено важливість масштабованості, точності та адаптивності методів у мінливих умовах мережі. Дослідження актуальне через зростання популярності пірингових технологій і необхідність підвищення їхньої безпеки. Узагальнення знань у цій сфері сприятиме розробці нових рішень для забезпечення стійкості та надійності децентралізованих систем.

Ключові слова: децентралізована система, пірингова мережа, комп'ютерна мережа, виявлення аномалій, кібербезпека, загроза безпеці, машинне навчання, моніторинг трафіку, захист мережі.

.

LUZHETSKYI Volodymyr, SAVYTSKA Liudmyla
Vinnytsia National Technical University

ANALYSIS OF ANOMALIES DETECTION APPROACHES IN DECENTRALIZED COMPUTER NETWORKS

In the article a review of contemporary approaches to anomaly detection in decentralized peer-to-peer (P2P) networks is presented. The challenges posed by the architectural features of P2P systems are examined, including the absence of centralized control, the diverse behavioral characteristics of nodes, and the necessity to preserve user privacy. The study focuses on analyzing methods used for monitoring network activity and identifying potential threats, such as denial-of-service attacks, botnets, unauthorized access, and malware distribution. Traditional approaches are discussed, including rule-based methods, statistical models, machine learning algorithms, graph theory-based techniques, and blockchain-based methods. The advantages and limitations of each approach, as well as their effectiveness in various scenarios, are highlighted. Rule-based methods are noted for their efficiency in detecting known attacks but lack adaptability to unknown threats. In contrast, ML algorithms can uncover hidden patterns but require substantial computational resources. Graph theory-based methods facilitate the analysis of network structures to detect anomalies, though their implementation in large-scale networks remains challenging. The article also provides examples of successful implementations, such as the decentralized monitoring system GNUnet, and evaluates their strengths and weaknesses. Issues related to scalability, detection accuracy, and adaptability to dynamic network conditions are discussed in detail. The relevance of this research is driven by the growing popularity of P2P technologies and the increasing need to enhance their security. Summarizing the knowledge in this domain will contribute to the development of new methodologies and technological solutions for anomaly detection, ensuring the resilience and reliability of decentralized networks in the modern cyberspace.

Keywords: decentralized system, peer-to-peer network, computer network, anomaly detection, cybersecurity, security threat, machine learning, traffic monitoring, network protection.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК З ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Однорангові (peer-to-peer, P2P) децентралізовані мережі протягом останніх десятиліть зазнали значного розвитку та стали основою для багатьох сучасних технологій, таких як блокчейн, розподілені файлові системи, системи обміну контентом та інші. Їхня децентралізована архітектура забезпечує високу стійкість до відмов, масштабованість та відсутність єдиного контрольного центру, що робить їх привабливими для широкого спектра застосувань [1, 2].

Однак, саме відкритий та децентралізований характер P2P мереж робить їх вразливими до різноманітних кіберзагроз. Зловмисні вузли можуть легко інтегруватися в мережу, маскуючись під легітимних учасників. Вони можуть здійснювати атаки типу "відмова в обслуговуванні" (DoS), розповсюджувати шкідливе програмне забезпечення, маніпулювати даними або перехоплювати конфіденційну інформацію [3, 4]. Крім того, такі вузли можуть об'єднуватися, створюючи синергетичний ефект, що значно підвищує ризики для безпеки мережі.

Проблема виявлення шкідливих хостів у P2P мережах ускладнюється відсутністю централізованого контролю та необхідністю збереження приватності користувачів. Традиційні методи моніторингу та захисту, розроблені для централізованих мереж, не завжди можуть бути застосовані в децентралізованому середовищі. Це зумовлює потребу у спеціалізованих підходах до виявлення аномалій, які враховують особливості P2P архітектури та поведінки вузлів.

Аномалії в мережі можуть проявлятися у вигляді незвичної активності, відхилення від стандартних патернів трафіку або поведінки вузлів. Вчасне та точне виявлення таких аномалій є критично важливим для запобігання потенційним атакам, забезпечення цілісності та конфіденційності даних, а також підтримання надійної роботи мережі. Це особливо актуально в контексті зростання кількості кіберзагроз та збільшення залежності сучасних систем від P2P технологій [4-6].

Актуальність виявлення аномалій у P2P мережах полягає не лише в захисті від поточних загроз, але й у забезпеченні стійкості мережі до майбутніх атак. Це сприяє підвищенню довіри користувачів до децентралізованих систем та стимулює подальший розвиток інноваційних технологій на їх основі.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою дослідження є проведення огляду існуючих підходів щодо виявлення аномалій у однорангових децентралізованих мережах, визначення основних напрямків досліджень у цій галузі, аналіз основних ідей та результатів ключових наукових робіт. Це дозволить сформувати цілісне уявлення про сучасний стан проблеми та окреслити перспективні напрямки подальших досліджень.

Актуальність такого огляду зумовлена необхідністю узагальнення та систематизації знань у цій сфері, яка швидко розвивається. В умовах постійного зростання складності та масштабів P2P мереж, а також еволюції методів атак, дослідники та практики потребують актуальної інформації про ефективні методи виявлення аномалій. Це сприятиме підвищенню рівня безпеки мереж, розвитку нових технологічних рішень та встановленню стандартів у галузі кібербезпеки децентралізованих систем.

ПРОБЛЕМИ ВИЯВЛЕННЯ АНОМАЛІЙ В ОДНОРАНГОВИХ МЕРЕЖАХ

Методи виявлення аномалій в P2P мережах мають вирішальне значення для виявлення нестандартних шаблонів і поведінки вузлів, що може вказувати на потенційні загрози безпеці, такі як несанкціонований доступ або присутність зловмисних однорангових користувачів. У децентралізованій архітектурі P2P-мережі забезпечують прямий зв'язок між користувачами без централізованого управління, що підвищує масштабованість і ефективність, але також створює унікальні вразливості, якими можуть скористатися зловмисники [3, 7].

Виявлення аномалій в P2P мережах створює унікальні проблеми через децентралізовану природу цих систем і складну взаємодію між вузлами. Розуміння цих проблем має вирішальне значення для розробки ефективних технологій виявлення.

Однією з важливих проблем при виявленні аномалій є виникнення помилкових їх визначень. Аномалії визначаються як відхилення від нормальної поведінки, але властивий мережевому трафіку шум може приховати справжні аномалії і призвести до помилкових класифікацій [8]. Наприклад, неочікувана передача великих обсягів даних може викликати хибні тривоги, ускладнюючи процес виявлення [9]. Ця проблема поширена як в системах машинного навчання, так і для ручного моніторингу, що вимагає надійних методів для розпізнавання справжніх загроз і «доброякісних» аномалій.

P2P-мережі демонструють різноманітні поведінкові характеристики, які можуть сильно відрізнятися залежно від застосування і взаємодії користувачів. Як наслідок, визначення того, що є «нормальною» поведінкою, стає складним завданням. В деяких дослідженнях пропонується використовувати передові методи машинного навчання для аналізу потоку мережевого трафіку, що дозволяє ідентифікувати патерни, які вказують на наявність бот-мереж та інших аномалій [10]. Однак створення алгоритмів для точного відображення цих взаємодій при мінімізації ризику помилкових спрацьовувань залишається актуальною проблемою [11].

Великий обсяг даних у P2P-мережах ускладнює виявлення аномалій. Багато існуючих методів стикаються з труднощами при роботі з наборами даних, що перевищують сотні тисяч елементів, що робить масштабованість критично важливим питанням [12]. Для ефективного вирішення проблем, пов'язаних з великими даними, було розроблено методи на основі розподілених обчислень, такі як Apache Spark. Ці платформи сприяють обробці складних, високорозмірних наборів даних, дозволяючи ідентифікувати аномалії, зберігаючи при цьому ефективність [12]. Тому необхідні постійні вдосконалення, щоб забезпечити здатність цих методів встигати за мінливою поведінкою мережі.

Ефективне виявлення аномалій вимагає постійного моніторингу мережевої активності для своєчасного виявлення загроз. Динамічний характер P2P-мереж означає, що їхня поведінка може швидко змінюватися, що зумовлює необхідність механізмів виявлення в реальному часі. Моніторинг мережі має проводитися постійно для зменшення потенційних загроз, таких як програми-вимагачі, DDoS-атаки та

несанкціонований доступ [9, 13]. Впровадження систем, здатних адаптуватися та реагувати на дані в реальному часі, є важливим для підвищення безпеки в P2P-мережах.

Інтеграція знань про предметну область, таких як приналежність до спільноти всередині мережі, може покращити точність виявлення аномалій. Ймовірнісні моделі, що враховують цю інформацію, допомагають у визначенні закономірностей взаємодії та ефективнішому виявленні відхилень [14]. Однак, розробка таких моделей вимагає глибокого розуміння архітектури мережі та взаємодії між її компонентами, що може бути ресурсомістким процесом.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА МЕТОДІВ ВИЯВЛЕННЯ АНОМАЛІЙ В ДЕЦЕНТРАЛІЗОВАНИХ МЕРЕЖАХ

Для виявлення аномалій в децентралізованих мережах використовуються різноманітні методи, починаючи від простих методів на основі правил та статистичних методів і закінчуючи складними алгоритмами глибокого машинного навчання.

Методи виявлення аномалій, засновані на правилах, базуються на заздалегідь визначених правилах або сигнатурах для ідентифікації аномальної поведінки в мережах [15, 16]. Вони найчастіше використовуються для моніторингу трафіку, перевірки відповідності протоколам і виявлення специфічних шаблонів аномалій. Ці методи ефективні для виявлення відомих атак, таких як розподілені атаки типу DDoS чи поширення шкідливого програмного забезпечення. Їх перевагами є простота реалізації та інтерпретованість, що дозволяє швидко впроваджувати нові правила. Однак їх основний недолік полягає в низькій адаптивності: методи не можуть ідентифікувати нові, невідомі загрози, і потребують постійного оновлення правил. Ці обмеження роблять їх ефективними лише в умовах стабільного та передбачуваного середовища.

Статистичні методи використовують моделі нормальної поведінки, засновані на аналізі даних про трафік або дії вузлів у мережі [17]. Відхилення від статистичних норм розглядається як потенційна аномалія. Ці методи добре підходять для виявлення аномалій типу перевантаження мережі або тривалих аномалій в обміні даними. Основними перевагами є здатність адаптуватися до змін у звичайному поведінковому профілі мережі та чіткі порогові значення для визначення аномалій. Недоліками є схильність до високого рівня хибнопозитивних спрацьовувань і потреба у великій кількості якісних даних для коректної побудови моделей.

Методи машинного навчання (ML) включають як контрольоване навчання, так і неконтрольовані алгоритми для аналізу шаблонів поведінки у мережі [14, 18]. Вони дозволяють виявляти як відомі, так і невідомі загрози. Унікальність ML-методів полягає в їхній здатності навчатися на великих наборах даних і знаходити приховані кореляції, недоступні для традиційних методів. Прикладами використання є виявлення шкідливого програмного забезпечення у P2P-системах або попередження витоків даних. Однак такі методи є ресурсомісткими, вимагають значних обчислювальних потужностей і якісного навчального набору даних, що може бути проблемою в динамічних децентралізованих мережах.

Методи, що базуються на теорії графів, представляють мережу як граф, де вузли є вершинами, а зв'язки між ними – ребрами. Аномалії виявляються через аналіз структури графа, наприклад, центральності, щільності кластерів або відхилень у комунікаційних шаблонах [19, 20]. Такі методи особливо ефективні для виявлення атак типу Сібілли, де зловмисники створюють велику кількість підроблених вузлів для порушення функціонування мережі. Переваги цих методів полягають у їхній здатності візуалізувати та аналізувати структуру мережі. Однак складність обробки великих графів і потреба у високій обчислювальній потужності є значними недоліками.

Методи, засновані на блокчейні, використовують децентралізований і незмінний характер блокчейнів для підвищення безпеки та прозорості в процесі виявлення аномалій. Вони можуть забезпечити точний запис підозрілих дій у мережі, використовуючи смарт-контракти для автоматичного моніторингу та реагування на аномалії [21, 22]. Ці методи особливо підходять для виявлення маніпуляцій даними в P2P-блокчейнах. Основними перевагами є підвищена стійкість до втручання зловмисників і можливість використання у динамічних середовищах. Недоліки включають високі витрати на обчислення, потребу в додаткових ресурсах для зберігання даних та затримки в часі через необхідність перевірки транзакцій.

АНАЛІЗ ДОСЛІДЖЕНЬ ЩОДО ВИЯВЛЕННЯ АНОМАЛІЙ В ДЕЦЕНТРАЛІЗОВАНИХ МЕРЕЖАХ

У дослідженні [23] представлено децентралізовану систему моніторингу GNUnet для виявлення аномалій. У цьому підході використовуються сенсори для збору даних про активність вузлів і натренована гаусівська модель для ідентифікації відхилень від нормальної поведінки. Сильними сторонами цього підходу є його автономність і здатність функціонувати без централізованого управління. Однак аналіз показує, що пропоноване авторами рішення може бути ресурсовитратним, що обмежує його застосування у великих або динамічних мережах. Дослідження також демонструє, що такий підхід ефективний у випадках короткотривалих аномалій та потребує подальшого вдосконалення для аналізу довготривалих складних сценаріїв, що включають комбіновані атаки

Автори роботи [24] фокусується на дослідженні впливу P2P трафіку на роботу систем виявлення аномалій та пропонують підхід для зменшення цього впливу. Основна ідея полягає в попередній фільтрації P2P трафіку перед його аналізом системою виявлення аномалій. Перед подачею трафіку на систему виявлення аномалій, він пропускається через класифікатор, який визначає, чи є трафік P2P, чи ні. Система виявлення аномалій аналізує лише не-P2P трафік, що дозволяє уникнути помилкового визначення аномалій, спричинених особливостями P2P трафіку. Фільтрація P2P трафіку дозволяє уникнути помилкових спрацьовувань, викликаних схожістю деяких характеристик P2P трафіку з аномальною активністю. Ефективність рішення безпосередньо залежить від якості класифікатора. Якщо класифікатор помилково класифікує аномальний трафік як P2P, то він не буде виявлений. Автори самі визнають, що існуючі на момент написання статті класифікатори були недостатньо точними, особливо для зашифрованого P2P трафіку. Крім того, запропонований підхід не вирішує проблему виявлення аномалій, які відбуваються всередині P2P мереж (наприклад, поширення шкідливого ПЗ через P2P мережі), а також фільтрація трафіку може вимагати значних обчислювальних ресурсів, особливо при великих обсягах трафіку.

Дослідження [25] присвячене використанню довірених вузлів для моніторингу поведінки сусідів у піринговых потокових мережах. Основна ідея полягає у створенні моделі репутації, яка враховує регулярні звіти про поведінку сусідів. Моніторингові вузли організовуються у двійкове дерево, що забезпечує балансування навантаження. Цей підхід демонструє високу точність і низький рівень хибних спрацювань, але покладається на наявність довірених вузлів. Це створює потенційну вразливість, адже компрометація одного або декількох довірених вузлів може значно знизити ефективність системи. Моніторинговий трафік також може створювати значне навантаження на мережу, особливо в умовах великої кількості вузлів.

У роботі [26] розглядається статистичний підхід на основі χ^2-аналізу для виявлення P2P-ботнетів. Основна ідея підходу полягає в аналізі часових характеристик трафіку (тривалості та часових слотів) для виявлення присутності бот-сервера. Він дозволяє точно виявляти ботнети, що використовують методи маскування. Перевагами цього підходу є його здатність виявляти складні аномалії з низьким рівнем хибних спрацювань. Однак він вимагає великих обчислювальних ресурсів, що може обмежувати його використання в реальному часі. Крім того, підхід обмежений у здатності адаптуватися до нових типів атак без додаткової оптимізації. Автори зосереджуються лише на часових характеристиках трафіку, ігноруючи інші важливі параметри, такі як обсяг трафіку, кількість з'єднань, географічне розташування вузлів тощо. Більш повний аналіз, що враховує різноманітні характеристики трафіку, може покращити точність виявлення. Також для ефективної роботи запропонованого авторами методу необхідно правильно визначити порогові значення для χ^2-статистики. Це може бути складно, особливо в динамічних P2P мережах.

В іншому дослідженні [27] пропонується фреймворк довіри для P2P мереж, який поєднує репутаційний механізм з технікою виявлення аномалій на основі профілів пірів. У цьому підході профіль поведінки створюється на основі історичних даних активності вузла, а відхилення від нормальної поведінки знижують його репутацію. Для кожного піра створюється профіль, який описує його типову поведінку в мережі (час з'єднання, тривалість сесії, кількість запитів, завантажень, відвантажень тощо). Система спостерігає за активністю пірів та порівнює її з їхніми профілями. Якщо поведінка піра відхиляється від норми, то це визначається як аномалія. Аномальна поведінка впливає на репутацію піра. Чим більше аномалій, тим нижча репутація. Репутаційна система та механізм виявлення аномалій інтегровані у єдиний фреймворк довіри. Піри з низькою репутацією можуть бути ізольовані або обмежені в своїх діях. Виявлення аномалій дозволяє враховувати не лише минулу поведінку піра, але й його поточну активність, що робить оцінку довіри більш точною. Репутація піра оновлюється не тільки після завершення сесії, а й під час її виконання, що дозволяє швидко реагувати на зміни в його поведінці. Серед недоліків можна відзначити те, що створення точних та актуальних профілів пірів може бути складним завданням, особливо в динамічних P2P мережах. Зловмисники можуть намагатися маніпулювати профілями пірів, щоб уникнути виявлення або знизити репутацію інших пірів. Моніторинг активності пірів та аналіз аномалій можуть вимагати значних обчислювальних ресурсів. Поєднання репутаційного механізму з виявленням аномалій дозволяє більш точно оцінювати довіру до пірів та виявляти приховані загрози. Однак, для практичного застосування цього підходу необхідно вирішити проблеми, пов'язані зі складністю побудови профілів, хибнопозитивними спрацьовуваннями та ресурсоємністю.

Робота [28] присвячена методам виявлення змови, а саме аномальних користувачів, що незаконно поширюють платний контент у піринговых мережах доставки контенту. Методи базуються на системі репутації, де піри оцінюють один одного та надсилають звіти до централізованого сервера управління. В першому методі піри періодично надсилають звіти про поведінку своїх сусідів, вказуючи, чи намагалися сусіди створити незаконний кластер для обміну контентом. Сервер періодично вибирає деяких пірів як підставних та просить їх імітувати поведінку змовників. Сусіди, що погоджуються на створення незаконного кластера з підставним піром, отримують негативні оцінки. Репутація піра розраховується на основі отриманих звітів, зважених за репутацією тих, хто їх надіслав. Піри з низькою репутацією вважаються аномальними. Другий метод доповнює перший та використовує модель PMC (Preparata-Metze-Chien) для підвищення точності виявлення аномалій. Якщо пір A вважає піра B надійним, а пір B вважає

піра С надійним, то пір А транзитивно вважає піра С надійним. Сервер визначає максимальну групу пірів, які вважають один одного надійними. Всі піри поза цією групою вважаються аномальними. Перевагою запропонованих рішень є висока точність виявлення особливо другим методом. Сервер збирає та аналізує звіти, що спрощує управління системою репутації. Серед недоліків можна відзначити те, що перший метод можна обійти, якщо змовники будуть координувати свої дії та надсилати неправдиві звіти. Другий метод частково вирішує цю проблему, але все ще має деяку вразливість. Також другий метод потребує певної кількості звітів перед початком аналізу, що може призвести до затримки у виявленні аномалій.

У дослідженні [29] автори пропонують фреймворк для виявлення та захисту від DDoS-атак у розподілених піринговых мережах. Фреймворк використовує значення TTL та відстань між джерелом та жертвою для виявлення аномалій, характерних для DDoS-атак. Спеціальний агент збирає інформацію про вузли, їхню пропускну здатність та інші параметри для ефективного відстеження атак. При виявленні підозрілої активності (наприклад, великої кількості запитів) на стороні жертви, вона надсилає запит до агента. Агент аналізує TTL пакетів та відстань між джерелом та жертвою. Різниця у значеннях TTL для пакетів, що нібито походять з одного джерела, може свідчити про підробку адрес та DDoS-атаку. На стороні джерела встановлюється обмеження швидкості трафіку для запобігання перевантаженню жертви. Агент моніторить трафік та динамічно змінює обмеження швидкості в залежності від інтенсивності атаки. Після завершення атаки обмеження швидкості скасовується. Серед переваг запропонованого підходу є те, що TTL дозволяє ефективно виявляти DDoS-атаки, що використовують підробку адрес. Крім того, захист реалізується на крайових маршрутизаторах, що дозволяє розподілити навантаження та підвищити стійкість до атак. Недоліками такого методу є те, що точність вимірювання TTL може впливати на ефективність виявлення атак. При цьому нормальний трафік з різними значеннями TTL може бути помилково класифікований як DDoS-атака. Також агент є централізованою точкою відмови.

Автори роботи [30] досліджують методи машинного навчання для виявлення різноманітних аномалій в децентралізованих мережах типу «блокчейн». Досліджуються різні методи неконтрольованого навчання. Аналіз показав що досить часто використовуються для виявлення аномалій метод k-середніх, DBSCAN,one-class SVM, а також нейронні генеративні змагальні мережі. Автори пропонують класифікацію методів виявлення аномалій на три категорії: методи, що використовують лише неконтрольоване навчання; методи, що комбінують кілька алгоритмів неконтрольованого навчання; методи, що поєднують неконтрольоване та контрольоване навчання. Підкреслюється важливість генеративного штучного інтелекту для розв'язання проблеми асоціації адрес з користувачами та покращення точності і масштабованості кластерного аналізу. Вибір найкращого методу залежить від конкретної задачі та вимог до точності, швидкості та ресурсів. В деяких випадках може бути доцільним комбінувати різні методи для досягнення оптимальних результатів. Важливо також враховувати еволюцію блокчейну та адаптувати методи до нових типів аномалій та атак.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У цьому дослідженні було розглянуто важливість та виклики виявлення аномалій у динамічних середовищах децентралізованих мереж. Перспективними напрямками розвитку є оптимізація моделей, а також розробка гібридних підходів, що поєднують сильні сторони різних алгоритмів, а також застосування методів глибокого навчання, зокрема навчання з частковим наглядом, особливо враховуючи обмеженість маркованих даних. Також перспективним підходом щодо виявлення аномалій в піринговых мережах може бути використання методів машинного навчання з підкріпленням завдяки своїй здатності адаптуватися до динамічної та складної природи цих мереж.

З огляду на зростання інтенсивності кіберзагроз, критично важливим є створення надійних систем виявлення аномалій у реальному часі, здатних протистояти атакам типу DDoS. Подальші дослідження повинні бути зосереджені на розробці алгоритмів для обробки потоків даних у реальному часі, що дозволить швидко реагувати на аномалії та мінімізувати потенційні збитки. Розвиток цих напрямків сприятиме значному покращенню безпеки та надійності децентралізованих мереж.

Література

1. Global Peer-to-peer Network Market Size. 2023. URL: https://www.globalmarketestimates.com/market-report/peer-to-peer-network-market-4294
2. Куперштейн Л.М., Кренцін М.Д. Аналіз тенденцій розвитку пірингових мереж. *Вісник ХНУ. Технічні науки*. 2021. Т. 299, №4. С. 26–29. URL: https://doi.org/10.31891/2307-5732-2021-299-4-26-29
3. Куперштейн Л.М., Кренцін М.Д., Дудатьєв А.В., Каплун В.А. Аналіз проблем безпеки пірінгових мереж. *Інформаційні технології та комп'ютерна інженерія*. 2022. Т. 54, № 2. С. 5–14. URL: https://doi.org/10.31649/1999-9941-2022-54-2-5-14
4. Security in peer-to-peer connections: advantages and risks. URL: https://negg.blog/en/security-in-peer-to-peer-connections-advantages-and-risks
5. The evolution of P2P transactions: a comprehensive guide. URL: https://innowise.com/blog/peer-to-peer-transactions

6. How has the Rise of P2P Payment Systems Impacted the Way Society Handles Money. URL: https://fintechloom.com/how-has-the-rise-of-p2p-payment-systems-impacted-the-way-society-handles-moneyociety-handles-money

7. Eisenbarth, J.-P., Cholez, T., & Perrin, O. Ethereum's Peer-to-Peer Network Monitoring and Sybil Attack Prevention. *Journal of Network and Systems Management*, 2022, 30(65). URL: https://doi.org/10.1007/s10922-022-09676-2

8. Марченко Р., Коваленко А., Знайдюк В. Аналіз методів виявлення аномального трафіку в мережах IoT. *Системи управління, навігації та зв'язку. Збірник наукових праць*. 2024. Т. 1, № 75. С. 133–136. URL: https://doi.org/10.26906/sunz.2024.1.133

9. Evaluating Anomaly Detection Techniques In Data Quality Assurance. URL: https://peerdh.com/blogs/programming-insights/evaluating-anomaly-detection-techniques-in-data-quality-assurance

10. Harnoorkar S. A Study of Anomaly Detection Techniques. *International Journal for Research in Applied Science and Engineering Technology*. 2020. Vol. 8, no. 6. P. 960–962. URL: https://doi.org/10.22214/ijraset.2020.6155

11. Azmi M. F., Karim H. A., AlDahoul N. Anomaly Detection for Network Security. *International Journal of Membrane Science and Technology*. 2023. Vol. 10, no. 1. P. 299–316. URL: https://doi.org/10.15379/ijmst.v10i1.1808

12. A comprehensive survey of anomaly detection techniques for high dimensional big data / S. Thudumu et al. *Journal of Big Data*. 2020. Vol. 7, no. 1. URL: https://doi.org/10.1186/s40537-020-00320-x

13. Duraj A. Anomaly detection in network traffic. *PRZEGLĄD ELEKTROTECHNICZNY*. 2022. Vol. 1, no. 12. P. 207–210. URL: https://doi.org/10.15199/48.2022.12.46

14. Hooshmand M. K., Hosahalli D. Network anomaly detection using deep learning techniques. *CAAI Transactions on Intelligence Technology*. 2022. URL: https://doi.org/10.1049/cit2.12078

15. Gowri M., Paramasivan B. Rule-Based Anomaly Detection Technique Using Roaming Honeypots for Wireless Sensor Networks. *ETRI Journal*. 2016. Vol. 38, no. 6. P. 1145–1152. URL: https://doi.org/10.4218/etrij.16.0115.0795

16. Chen C.-L., Chen H.-C. A Hybrid Approach Combining Rule-Based and Anomaly-Based Detection Against DDoS Attacks. *International Journal of Network Security & Its Applications*. 2016. Vol. 8, no. 5. P. 1–18. URL: https://doi.org/10.5121/ijnsa.2016.8401

17. Радівілова Т.А., Кіріченко Л.О., Тавалбех М.Х., Ільков А.А. Виявлення аномалій втелекомунікаційномутрафіку статистичними методами /*Кібербезпека: освіта, наука, техніка.* 2021. №3 (11). С. 183-194. URL: https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/247/221

18. Sayed A. K. Anomaly Detection Using Machine Learning. *IJARCCE*. 2023. Vol. 12, no. 1. URL: https://doi.org/10.17148/ijarcce.2023.12103

19. Threat Identification and Examination using Graph Based Anomaly Detection. International Journal of Engineering and Advanced Technology. 2019. Vol. 9, no. 1. P. 7510–7513. URL: https://doi.org/10.35940/ijeat.a3129.109119

20. Visualization of Anomalies using Graph-Based Anomaly Detection / R. Paudel et al. The *International FLAIRS Conference Proceedings*. 2021. Vol. 34, no. 1. URL: https://doi.org/10.32473/flairs.v34i1.128554

21. Ko K.-M. Transaction Analysis based Blockchain Network Anomaly Detection. *The Journal of Korean Institute of Information Technology*. 2023. Vol. 21, no. 5. P. 131–137. URL: https://doi.org/10.14801/jkiit.2023.21.5.131

22. BAD: A Blockchain Anomaly Detection Solution / M. Signorini et al. *IEEE Access*. 2020. Vol. 8. P. 173481–173490. URL: https://doi.org/10.1109/access.2020.3025622

23. Tarabai O. A Decentralized and Autonomous Anomaly Detection Infrastructure for Decentralized Peer-to-Peer Networks. URL: https://www.net.in.tum.de/fileadmin/bibtex/publications/theses/tarabai2014decmon.pdf

24. Haq I. U., Ali S., Khan H., Khayam S. A. What Is the Impact of P2P Traffic on Anomaly Detection? // Proceedings of the 13th International Symposium on Recent Advances in Intrusion Detection (RAID 2010). – Berlin: Springer, 2010. – P. 1–17.

25. Jin X., Chan S. H. G. Detecting malicious nodes in peer-to-peer streaming by peer-based monitoring. *ACM Transactions on Multimedia Computing, Communications, and Applications*. 2010. Vol. 6, no. 2. P. 1–18. URL: https://doi.org/10.1145/1671962.1671965

26. Syahirah R., M. F., Azri Z. Multivariate Statistical Analysis on Anomaly P2P Botnets Detection. *International Journal of Advanced Computer Science and Applications*. 2017. Vol. 8, no. 12. URL: https://doi.org/10.14569/ijacsa.2017.081259

27. Trust Framework for P2P Networks Using Peer-Profile Based Anomaly Technique / N. Stakhanova et al. *25th IEEE International Conference on Distributed Computing Systems Workshops*, Columbus, OH, USA. URL: https://doi.org/10.1109/icdcsw.2005.137

28. Abdullah E., Fujita S. Reputation-Based Colluder Detection Schemes for Peer-to-Peer Content Delivery Networks. *IEICE Transactions on Information and Systems*. 2013. E96.D, no. 12. P. 2696–2703. URL: https://doi.org/10.1587/transinf.e96.d.2696

29. Jaideep G., Prakash Battula B. Detection of DDOS attacks in distributed peer to peer networks. *International Journal of Engineering & Technology*. 2018. Vol. 7, no. 2.7. P. 1051. URL: https://doi.org/10.14419/ijet.v7i2.7.12227

30. Anomaly Detection in Blockchain Networks Using Unsupervised Learning: A Survey / C. Cholevas et al. *Algorithms*. 2024. Vol. 17, no. 5. P. 201. URL: https://doi.org/10.3390/a17050201

References

1. Global Peer-to-peer Network Market Size. 2023. URL: https://www.globalmarketestimates.com/market-report/peer-to-peer-network-market-4294.

2. Kupershtein L., Krentsin M. Analysis of peer-to-peer networks trends. *Herald of khmelnytskyi national university*. 2021. Vol. 299, no. 4. P. 26–29. URL: https://doi.org/10.31891/2307-5732-2021-299-4-26-29.

3. Kupershtein L., Krentsin M. et al. Analysis of security problems of peer-to-peer networks. *Information technology and computer engineering*. 2022. Vol. 54, № 2. P. 5–14. URL: https://doi.org/10.31649/1999-9941-2022-54-2-5-14.
4. Security in peer-to-peer connections: advantages and risks. URL: https://negg.blog/en/security-in-peer-to-peer-connections-advantages-and-risks.
5. The evolution of P2P transactions: a comprehensive guide. URL: https://innowise.com/blog/peer-to-peer-transactions.
6. How has the Rise of P2P Payment Systems Impacted the Way Society Handles Money. URL: https://fintechloom.com/how-has-the-rise-of-p2p-payment-systems-impacted-the-way-society-handles-moneyociety-handles-money.
7. Eisenbarth, J.-P., Cholez, T., & Perrin, O. Ethereum's Peer-to-Peer Network Monitoring and Sybil Attack Prevention. *Journal of Network and Systems Management*, 2022, 30(65). URL: https://doi.org/10.1007/s10922-022-09676-2.
8. Marchenko R., Kovalenko A., Znaidiuk V. Analiz metodiv vyiavlennia anomalnoho trafiku v merezhakh IoT. *Systemy upravlinnia, navihatsii ta zv'iazku. Zbirnyk naukovykh prats*. 2024. T. 1, № 75. C. 133–136. URL: https://doi.org/10.26906/sunz.2024.1.133.
9. Evaluating Anomaly Detection Techniques In Data Quality Assurance. URL: https://peerdh.com/blogs/programming-insights/evaluating-anomaly-detection-techniques-in-data-quality-assurance
10. Harnoorkar S. A Study of Anomaly Detection Techniques. *International Journal for Research in Applied Science and Engineering Technology*. 2020. Vol. 8, no. 6. P. 960–962. URL: https://doi.org/10.22214/ijraset.2020.6155
11. Azmi M. F., Karim H. A., AlDahoul N. Anomaly Detection for Network Security. *International Journal of Membrane Science and Technology*. 2023. Vol. 10, no. 1. P. 299–316. URL: https://doi.org/10.15379/ijmst.v10i1.1808
12. A comprehensive survey of anomaly detection techniques for high dimensional big data / S. Thudumu et al. *Journal of Big Data*. 2020. Vol. 7, no. 1. URL: https://doi.org/10.1186/s40537-020-00320-x.
13. Duraj A. Anomaly detection in network traffic. *PRZEGLĄD ELEKTROTECHNICZNY*. 2022. Vol. 1, no. 12. P. 207–210. URL: https://doi.org/10.15199/48.2022.12.46.
14. Hooshmand M. K., Hosahalli D. Network anomaly detection using deep learning techniques. *CAAI Transactions on Intelligence Technology*. 2022. URL: https://doi.org/10.1049/cit2.12078.
15. Gowri M., Paramasivan B. Rule-Based Anomaly Detection Technique Using Roaming Honeypots for Wireless Sensor Networks. *ETRI Journal*. 2016. Vol. 38, no. 6. P. 1145–1152. URL: https://doi.org/10.4218/etrij.16.0115.0795 .
16. Chen C.-L., Chen H.-C. A Hybrid Approach Combining Rule-Based and Anomaly-Based Detection Against DDoS Attacks. *International Journal of Network Security & Its Applications*. 2016. Vol. 8, no. 5. P. 1–18. URL: https://doi.org/10.5121/ijnsa.2016.840.
17. Radivilova T.A., Kirichenko L.O., Tavalbekh M.Kh., Ilkov A.A. Vyiavlennia anomalii v telekomunikatsiinomu trafiku statystychnymy metodamy / *Kiberbezpeka: osvita, nauka, tekhnika*. 2021. №3 (11). C. 183-194. URL: https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/247/221.
18. Sayed A. K. Anomaly Detection Using Machine Learning. *IJARCCE*. 2023. Vol. 12, no. 1. URL: https://doi.org/10.17148/ijarcce.2023.12103.
19. Threat Identification and Examination using Graph Based Anomaly Detection. International Journal of Engineering and Advanced Technology. 2019. Vol. 9, no. 1. P. 7510–7513. URL: https://doi.org/10.35940/ijeat.a3129.109119.
20. Visualization of Anomalies using Graph-Based Anomaly Detection / R. Paudel et al. The International FLAIRS Conference Proceedings. 2021. Vol. 34, no. 1. URL: https://doi.org/10.32473/flairs.v34i1.128554 .
21. Ko K.-M. Transaction Analysis based Blockchain Network Anomaly Detection. *The Journal of Korean Institute of Information Technology*. 2023. Vol. 21, no. 5. P. 131–137. URL: https://doi.org/10.14801/jkiit.2023.21.5.131 .
22. BAD: A Blockchain Anomaly Detection Solution / M. Signorini et al. *IEEE Access*. 2020. Vol. 8. P. 173481–173490. URL: https://doi.org/10.1109/access.2020.3025622.
23. Tarabai O. A Decentralized and Autonomous Anomaly Detection Infrastructure for Decentralized Peer-to-Peer Networks. URL: https://www.net.in.tum.de/fileadmin/bibtex/publications/theses/tarabai2014decmon.pdf.
24. Haq I. U., Ali S., Khan H., Khayam S. A. What Is the Impact of P2P Traffic on Anomaly Detection? // Proceedings of the 13th International Symposium on Recent Advances in Intrusion Detection (RAID 2010). – Berlin: Springer, 2010. – P. 1–17.
25. Jin X., Chan S. H. G. Detecting malicious nodes in peer-to-peer streaming by peer-based monitoring. *ACM Transactions on Multimedia Computing, Communications, and Applications*. 2010. Vol. 6, no. 2. P. 1–18. URL: https://doi.org/10.1145/1671962.1671965.
26. Syahirah R., M. F., Azri Z. Multivariate Statistical Analysis on Anomaly P2P Botnets Detection. *International Journal of Advanced Computer Science and Applications*. 2017. Vol. 8, no. 12. URL: https://doi.org/10.14569/ijacsa.2017.081259.
27. Trust Framework for P2P Networks Using Peer-Profile Based Anomaly Technique / N. Stakhanova et al. *25th IEEE International Conference on Distributed Computing Systems Workshops*, Columbus, OH, USA. URL: https://doi.org/10.1109/icdcsw.2005.137.
28. Abdullah E., Fujita S. Reputation-Based Colluder Detection Schemes for Peer-to-Peer Content Delivery Networks. *IEICE Transactions on Information and Systems*. 2013. E96.D, no. 12. P. 2696–2703. URL: https://doi.org/10.1587/transinf.e96.d.2696.
29. Jaideep G., Prakash Battula B. Detection of DDOS attacks in distributed peer to peer networks. *International Journal of Engineering & Technology*. 2018. Vol. 7, no. 2.7. P. 1051. URL: https://doi.org/10.14419/ijet.v7i2.7.12227.
30. Anomaly Detection in Blockchain Networks Using Unsupervised Learning: A Survey / C. Cholevas et al. *Algorithms*. 2024. Vol. 17, no. 5. P. 201. URL: https://doi.org/10.3390/a17050201.