УДК 004.738.5:004.056.5
Неласа Г.В.[1], Орловський Д.І.[2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] студ. гр. РТ-812м. НУ «Запорізька політехніка»

ДЕАНОНІМІЗАЦІЯ В ОДНОРАНГОВИХ МЕРЕЖАХ: АНАЛІЗ СПОСОБІВ І ПРИКЛАДИ НА БАЗІ ПРОТОКОЛУ BITTORRENT

P2P мережі, або однорангові мережі, є системами, в яких кожен учасник може виконувати роль і клієнта, і сервера без необхідності проміжного сервера.

В сучасному світі P2P мережі використовуються в багатьох сферах – системах потокового відео, системах файлообміну, а особливе місце у сфері інтернет-фінансах. Вони стали основою для криптовалют, таких як Біткоїн, що забезпечують анонімність та безпеку фінансових операцій для користувачів.

Також P2P мережі можуть бути використані для створення децентралізованих фінансових систем (DeFi), які забезпечують надійність та прозорість транзакцій.

Основна ідея BitTorrent, популярної та широко використовуємої P2P системи для обміну файлами, полягає в тому, щоб розбити файли на безліч невеликих фрагментів та розподілити їх між учасниками мережі, які можуть

обмінюватись цими фрагментами один з одним. Таким чином відбувається розподіл навантаження на мережу.

Структура BitTorrent складається з наступних компонентів:

Торрент-файл – це невеликий файл, який містить метадані про файл (та інформацію про трекер, який координує обмін даними між учасниками мережі;

Трекер – сервер, який відповідає за забезпечення зв'язку між учасниками мережі. Трекер не зберігає самі файли, а лише координує обмін ними між учасниками рою;

Рій учасників мережі (peer's) – це користувачі, які беруть участь в обміні файлами. Діляться на: сідерів (завантажили повністю файл) та лічерів (завантажують, але не мають повної копії файлу);

Принцип роботи BitTorrent полягає у виконанні наступних шагів:

Користувач, який бажає завантажити файл, спочатку завантажує торрент-файл з Інтернету.

За допомогою торрент-клієнта користувач підключається до трекера, вказаного в торрент-файлі, і відправляє запит на отримання списку учасників мережі, які мають фрагменти файлу (сідери або лічери).

Трекер відправляє список peer's, і торрент-клієнт починає обмінюватися даними з ними. Фрагменти файлу завантажуються не послідовно, а у довільному порядку, щоб оптимізувати процес обміну даними між учасниками мережі.

У процесі завантаження файлу користувач також починає роздавати вже завантажені фрагменти іншим учасникам мережі. Це принцип «скооперованості» (tit-for-tat), який стимулює користувачів роздавати файли та забезпечує рівномірний розподіл навантаження.

Коли користувач завантажує всі фрагменти файлу, його торрент-клієнт автоматично збирає їх в один файл. У цей момент користувач стає сідером і продовжує роздавати файл іншим учасникам мережі.

Однак така структура мережі може бути використана для деанонімізації користувачів. Через відкриту природу P2P-мереж учасники мережі можуть бачити IP-адреси один одного, що може бути використано зловмисниками або правоохоронними органами для визначення справжніх ідентифікаторів користувачів та їхнього географічного розташування.

Деанонімізація користувачів в однорангових мережах, таких як BitTorrent, полягає у визначенні їхніх справжніх ідентифікаторів, таких як IP-адреса, географічне розташування або інші персональні дані. Існує кілька методів, які можуть бути використані для деанонімізації користувачів у мережах P2P:

Аналіз трафіку: зловмисники можуть перехоплювати та аналізувати мережевий трафік між учасниками мережі, щоб деанонімізувати учасників.

Статистична кореляція: збір та аналіз великої кількості даних про мережевий трафік та поведінку користувачів може дозволити виявити закономірності та встановити зв'язок між різними учасниками мережі.

Створення та використання мережевих «зондів»: зловмисники можуть створювати фальшиві учасників мережі (зонди), які збирають інформацію про справжніх учасників та передають її зловмисникам.

Атаки Sybil: атакуючий створює велику кількість фальшивих учасників мережі, щоб отримати контроль над великою частиною мережі та збирати інформацію про інших учасників.

Для забезпечення анонімності та захисту від деанонімізації користувачі можуть використовувати VPN-сервіси або проксі-сервери, які приховують реальні IP-адреси користувачів. Також, можна використовувати технології шифрування та анонімності, такі як Tor.

Деанонімізація користувачів в однорангових мережах, таких як BitTorrent, є актуальною проблемою, пов'язаною з приватністю та анонімністю. У статті було розглянуто різні методи деанонімізації та запропоновано заходи захисту, які можуть допомогти користувачам забезпечити свою приватність під час використання BitTorrent та інших мереж P2P.