УДК 004.75, 003.26

ДЕЦЕНТРАЛІЗОВАНА СИСТЕМА ОЦІНКИ ЯКОСТІ IOC НА ОСНОВІ БЛОКЧЕЙНУ З ВИКОРИСТАННЯМ МЕХАНІЗМУ КОНСЕНСУСУ Proof-of-Reputation

А. А. Бондаренко[1,a]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

Ця стаття пропонує децентралізоване блокчейн-рішення з використанням протоколу консенсусу Proof-of-Reputation для підвищення якості та надійності індикаторів компрометації. Для кількісної оцінки надійності учасників, які надають IOC в мережу, запроваджується динамічна рейтингова система на основі репутації, причому рейтинги поступово знижуються з часом для застарілих індикаторів. Оцінки IOC інтегровані в протокол PoRep, що стимулює високу репутацію, надаючи більшої ваги учасникам з високим рейтингом при перевірці та додаванні нових даних IOC до децентралізованого реєстру. Такий підхід сприяє обміну точною і своєчасною інформацією про загрози, одночасно систематично видаляючи з часом неактивних або скомпрометованих учасників з низькою репутацією.

Ключові слова: блокчейн, індикатори компрометації, proof-of-reputation, IOC

Вступ

В епоху постійних кіберзагроз, де загрози стають дедалі складнішими та поширенішими створюючи значні ризики для окремих осіб, організацій та критичної інфраструктури, своєчасне виявлення та реагування на інциденти є критичним завданням. Індикатори компрометації (indicator of compromise, IOC) відіграють ключову роль у цьому процесі, надаючи фахівцям цінні відомості про потенційні загрози. IOC – це будь-яка інформація, корисна для виявлення атаки. Сюди відносяться різноманітні артефакти чи сигнатури, які сприяють розпізнаванню атаки та її подальшої ідентифікації. Життєвий цикл IOC включає кілька етапів: формування/збирання-/відновлення переліку ознак компрометації, використання засобів моніторингу та виявлення для ідентифікації підозрілої активності, збирання даних про наявний IOC у середовищі, проведення аналізу для вивчення та навчання на основі цих IOC, а також вилучення застарілих IOC з використання.

Традиційні централізовані системи для оцінки та обміну даними про загрози мають певні обмеження, зокрема окремі точки відмови та відсутність прозорості. Щоб вирішити ці проблеми існує нагальна потреба в децентралізованій, стійкій і надійній системі, яка дає змогу ефективно обмінюватися і перевіряти IOC у спільноті кібербезпеки. Підвищення довіри до IOC вимагає їх оцінки за допомогою моделі оцінки, що враховує початкове значення, коефіцієнт розпаду та інші фактори. Різні типи IOC мають різну тривалість життєвого циклу – від днів для IP-адрес до років для геш-сум файлів.

Потреба у створенні децентралізованої системи оцінки якості IOC виникає через обмеження централізованих підходів. Централізовані системи вразливі до єдиної точки відмови, цензури та потенційних маніпуляцій з боку зловмисників. Крім того, їм часто бракує прозорості в процесах перевірки та розповсюдження IOC, що може підірвати довіру та ефективність.

Метою цієї роботи є запропонувати розв'язання проблеми різної якості та надійності наявних джерел IOC, пропонуючи децентралізовану систему на основі блокчейну з використанням механізму консенсусу Proof-of-Reputation (PoRep). Основна ідея полягає у впровадженні динамічної рейтингової системи IOC, яка кількісно оцінює надійність учасників, що надають IOC в мережу, з оцінками, призначеними для поступового зниження з часом для застарілих показників.

1. Модель оцінки

Модель [1] була розроблена для розрахунку довірчої оцінки (*trust* value) IOC протягом усього життєвого циклу. Для підрахунку $pulse_i$ (значення імпульсу для певного i-го IOC) була запропонована формула:

$$pulse_i = logistic(\sum_{j=1}^{N} trust_{ij}), \quad (1)$$

де $trust_{ij}$ – рівень довіри до j-го джерела імпульсів в діапазоні $(0, 1)$; N – кількість цих джерел;

[a]andbon-ipt22@lll.kpi.ua

$logistic(.)$ – функція нормалізації, яка приводить суму довіри декількох джерел до діапазону $(0, 1)$. І оскільки оцінка довіри також належить до того ж діапазону, значення імпульсу також нормалізується до $(0, 1)$.

Значення часу не можна недооцінювати, оскільки він безпосередньо впливає на спад індикатора або пов'язаних з ним довірчих інтервалів. Для тих інтервалів, де виявлено імпульси, метод визначення довірчої ймовірності полягає в наступному:

$$c_t = logistic(c_t^{decayed} + pulse_i), \tag{2}$$

де $c_t^{decayed}$ визначено як:

$$c_t^{decayed} = \frac{c_{t-1} - k * c_{t-1}(m - c_{t-1})}{m^2}, \tag{3}$$

$$f = \frac{a}{1 + \exp^{-k \cdot (b \cdot x - x_0)}}, \tag{4}$$

де c_t – рівень довіри в момент часу t; k – константа для регулювання швидкості спаду довіри відповідно до максимального терміну служби IOC; i – діапазон випадків/періодів. Варто зазначити, що рівняння (3) є скінченно-різницевою форма формою оберненої логістичної функції (рівняння (4) з $k < 0$ та $a = m$). У період відсутності імпульсних сигналів обчислення значення c_t визначається виключно за рівнянням (3).

2. Блокчейн

Proof-of-Reputation

Протокол консенсусу Proof-of-Reputation [2] спирається на авторитетність учасників для забезпечення безпеки мережі. Підписант блоку має володіти достатньо високим авторитетом, щоб у разі спроби обману системи зазнати значних фінансових та репутаційних втрат. Це поняття є доволі відносним, оскільки якщо компанію викриють у шахрайстві, то вона зазнає серйозних наслідків, однак великі компанії зазвичай ризикують більшим, ніж малі, тому перевага надається саме їм.

Після підтвердження авторитетності компанії та проходження верифікації, її включають до мережі як валідний вузол. З цього моменту вона функціонує як мережа Proof-of-Authority, де лише авторизовані вузли можуть підписувати та затверджувати блоки.

Для розв'язання проблеми різної якості джерел IOC, пропонуємо децентралізований підхід з використанням технології блокчейн і механізму консенсусу PoRep. Система включає динамічний рейтинг IOC, який кількісно оцінює надійність кожного учасника, що надає IOC в мережу. Важливо те, що рейтинг IOC користувача розроблений таким чином, щоб поступово знижуватися з часом, якщо не спостерігається подальшої шкідливої діяльності, імітуючи природне зниження актуальності застарілих індикаторів.

Рейтинг IOC, що зменшується з часом, інтегрований у консенсусний протокол PoRep, де учасники з вищою репутацією, що випливає з постійного надання високоякісних та оновлених даних IOC, отримують пропорційно більший вплив на перевірку та додавання нових даних IOC до децентралізованої книги обліку. Це заохочує постійне надання якісної інформації про загрози і водночас поступово усуває неактивних або скомпрометованих учасників, репутація яких погіршується. Прозорий, саморегульований характер запропонованої системи сприяє створенню стійкої, надійної екосистеми, яка забезпечує цілісність і надійність колективно використовуваних IOC, пом'якшуючи ризики, пов'язані з поширенням неточної або застарілої інформації.

Додатково, PoRep [3] не припускає, що майнери завжди гідні довіри, тому він потребує моніторингу дій майнерів та виключення зловмисних вузлів з мережі. PoRep пропонує механізми моніторингу та голосування, що мають на меті бути ефективнішими, ніж попередні механізми Byzantine Fault Tolerance (BFT). У PoRep найстаріші вузли мережі обираються для майнінгу згідно з критерієм зрілості. Майнери чергуються в круговому порядку для кожного нового блоку. Кожен майнер контролюється випадково вибраним журі, яке оцінює репутацію майнерів відповідно до порогу довіри, необхідного для мережі. Якщо репутація майнера нижча за поріг, журі голосує за виключення цього майнера. Крім того, механізм контролю доступу самостійно організовує мережу, змінюючи необхідну кількість майнерів, щоб підтримувати масштабованість мережі.

2.1. Атаки

2.1.1. Атака Double Spend

У мережі, заснованій на криптовалюті, зловмисник виконує дві майже послідовні транзакції з двома різними вузлами мережі. Наприклад, два платіжних перекази з сумами монет, що перевищують суму, яку зловмисник має в гаманці, але яка на момент переказів була підтверджена.

Стійкість до атаки Double Spend

Нехай зловмисник – це зловмисний вузол, який надсилає дві суперечливі транзакції одночасно, припускаючи, що одна з них буде недійсною.

Цей тип атаки пом'якшується, якщо транзакція буде ефективною тільки після того, як буде видобуто W блоків над блоком, який зберігав транзакцію. Крім того, геш-ланцюжок і розподілений блокчейн роблять малоймовірним визнання однієї з транзакцій недійсною. PoRep не заснований на конкуренції, тому кожен майнер додає мітку часу в кожен новий блок. Це гарантує, що малі форки трапляються рідко, але іноді все ж таки можуть статися. Якщо майнер зловживає своїми повноваженнями і спричиняє хаос, його виганяють. Випадкові форки вирішу-

ються за допомогою механізму Ethereum GHOST, а отже, маємо постійну узгодженість. Тому атаки подвійних витрат не відбуваються.

2.1.2. Атака 51%

Зловмисник повинен контролювати значну частину мережі, перш ніж впливати на механізм консенсусу. Атака, відома як «Атака 51%», вимагає, щоб користувач або група зі спільними інтересами контролювала щонайменше 51% потужності мережі для перевірки блоків.

Стійкість до 51% атаки

Нехай зловмисник є корумпованим користувачем, який контролює не менше 51% майнерів у мережі. При цьому зловмисник повинен дочекатися, поки його вузли стануть майнерами за критерієм зрілості. Припускаючи динамічне зростання мережі, зловмиснику може знадобитися ввести в мережу більше вузлів, щоб контролювати принаймні 51% майнерів, враховуючи, що легальні вузли також можуть стати майнерами під час атаки. Ця атака ускладнюється тим, що для того, щоб залишитися майнером після зловмисних дій, необхідно мати контроль над більш ніж половиною суддів кожного майнера. Це нездійсненно, оскільки судді вибираються випадковим чином, що вимагало б від зловмисника контролю майже всіх вузлів в мережі

2.1.3. Атака Impersonation

Зловмисник намагається отримати інформацію про конфігурацію або видати себе за майнера.

Стійкість до атаки Impersonation

Нехай зловмисник – це зловмисний вузол, який намагається видати себе за інший вузол. Його метою є модифікувати, пошкодити або створити транзакцію та/або блок, видаючи себе за інший вузол мережі.

Зловмисник може спробувати змінити або пошкодити транзакцію, перш ніж переслати її наступним вузлам. Однак це може статися лише з мізерно малою ймовірністю успішної підробки криптографічного підпису. Атаки, які шукають інформацію про конфігурацію, зменшуються завдяки шифруванню конфіденційної інформації. Таким чином, зловмисникам необхідно отримати приватний ключ передбачуваного одержувача. Крім того, запропонована модель дозволяє проводити аудит всіх минулих транзакцій. Тому, якщо зловмисник спробує модифікувати блокчейн за допомогою викраденої пари ключів, ця спроба буде зафіксована в журналі. Після виявлення зловмисника, вкрадені пари ключів можна легко видалити з мережі, відновивши безпечну роботу мережі та уникнувши подальшої шкоди.

2.1.4. Атака Selfish Miner

Зловмисник вибирає, які транзакції майнити, навмисно ігноруючи інші транзакції.

Стійкість до атаки Selfish Miner

Нехай зловмисник – зловмисний майнер, який вибирає транзакції для майнінгу та ігнорує інших у своєму раунді майнінгу.

Атака повинна тривати один раунд через ротацію майнінгу серед майнерів. Наступний легальний майнер в ротації буде видобувати найстаріші транзакції. Як тільки егоїстичний майнер буде виявлений, судді знизять його репутацію та/або проголосують за вигнання нападника

2.1.5. Атака Eclipse

Зловмисник намагається ізолювати вузол або групу вузлів, щоб перешкодити цільовим вузлам отримати поточне уявлення про мережеву активність і стан блокчейну.

Стійкість до атаки Eclipse

Нехай зловмисник – це зловмисний вузол, який знаходиться в стратегічній позиції в мережі і не пересилає транзакції та/або блоки наступним вузлам, намагаючись заперечити поточну версію блокчейну для інших вузлів.

Ця атака може бути пом'якшена в класичних мережах шляхом встановлення надлишкових шляхів між вузлами мережі. У нашій пропозиції припускається, що всі учасники з'єднані між собою як мінімум двома резервними шляхами в мережі.

2.1.6. Атака Denial of Service

Майнер може розглядатися як зловмисний вузол, якщо він навмисно відсутній в своєму раунді генерації блоків або не бере активної участі у функціоналі мережі.

Стійкість до атаки Denial of Service

Нехай зловмисник – майнер, який не виконує свої обов'язки. Відсутність може бути викликана збоєм у роботі вузла або відмовою майнера виконувати покладені на нього завдання.

У зловмисника є періодичний проміжок часу для видобутку нового блоку, але він утримується від цього. Всі судді чекають на новий блок, але він не з'являється у передбачуваний час. Таким чином, відсутність вузла майнера класифікується як зловмисна дія і обробляється запропонованим механізмом. Якщо час має вирішальне значення для заявки, одна відсутність може бути підставою для голосування за виключення

Висновки

У цій статті пропонується децентралізоване рішення на основі блокчейну з використанням консенсусного протоколу Proof-of-Reputation для вирішення проблеми різної якості та надійності існуючих джерел індикаторів компрометації. Основною ідеєю є впровадження динамічної рейтингової системи IOC, яка кількісно оцінює надійність учасників, що надають IOC до мережі. Рейтинги призначені для поступового зниження з часом для застарілих індикаторів. Ці оцінки IOC інтегровані в протокол PoRep, заохочуючи високу репутацію шляхом надання більшої ваги учасникам з високим рейтингом при перевірці та додаванні нових даних IOC до децентралізованого реєстру. Такий підхід сприяє обміну точними, актуальними даними про загрози, одночасно систематично видаляючи неактивних або скомпрометованих учасників з низькою репутацією з часом.

Додатково, у статті надається модель оцінки IOC та проаналізовано захист PoRep від атак подвійної витрати (Double Spend Attack), 51% атаки, атаки видавання себе за іншого (Impersonation Attack), атаки егоїстичного майнера (Selfish Miner Attack), затемнення мережі (Eclipse Attack) та атаки відмови в обслуговуванні (Denial of Service Attack).

Перелік використаних джерел

1. Indicators of compromise confidence scoring method / V. Tkach, O. Baranovskyi, A. Kudin, N. Godavarti, O. Kliok, S. Modali. — 2023. — URL: https://idaacs.digital/wp-content/uploads/2023/09/IDAACS23_PROCEEDINGS_VOL_1_new_3.pdf.
2. *Saini V.* ConsensusPedia: An encyclopedia of 30+ consensus algorithms / HackerNoon. — URL: https://hackernoon.com/consensuspedia-an-encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f.
3. Blockchain reputation-based consensus: A scalable and resilient mechanism for distributed mistrusting applications / M. T. de Oliveira, L. H. A. Reis, D. S. V. Medeiros, R. C. Carrano, S. D. Olabarriaga, D. M. F. Mattos // Comput. Netw. — 2020. — T. 179. — C. 107367. — DOI: 10.1016/j.comnet.2020.107367. — URL: https://doi.org/10.1016/j.comnet.2020.107367.