ВСТУП ДО ТЕХНОЛОГІЇ БЛОКЧЕЙН ТА КРИПТОВАЛЮТ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №1

"Захищеність від атак подвійних витрат у мережах з повільною синхронізацією"

1. Мета роботи

Дослідження особливостей атаки подвійних витрат.

2. Основні теоретичні відомості

Необхідні теоретичні відомості містяться в роботах:

1. *Lyudmila Kovalchuk, Dmytro Kaidalov, Andrii Nastenko, Mariia Rodinko, Oleksiy Shevtsov, Roman Oliynykov* Decreasing security threshold against double spend attack in networks with slow synchronization // Computer Communications, Volume 154, 2020, pp. 75-81, ISSN 0140-3664. doi: 10.1016/j.comcom.2020.01.079.a https://americanblockchainpac.org
2. *Lyudmila Kovalchuk, Mariia Rodinko, Roman Oliynykov, Dmytro Kaidalov, Andrii Nastenko* Probability of double spend attack for network with non-zero time delay // Publ. Math. Debrecen Supplementum 100, 2022, pp. 597-615. doi: 10.5486/PMD.2022.Suppl.4 https://konferencia.unideb.hu

3. Порядок і рекомендації щодо виконання роботи

Комп'ютерний практикум виконується бригадами, до складу яких входить до трьох студентів.

4. Завдання на комп'ютерний практикум

Розробити програмну реалізацію, яка дозволить провести відповідні обчислення:

Завдання 1. Обчислити поріг стійкості p_{st} (мінімальну частку зловмисних майнерів, яка гарантує, що ймовірність атаки подвійної витрати буде дорівнювати 1) для заданих значень інтенсивності створення блоків чесними майнерами α_H та зловмисними майнерами α_M.

Завдання 2. Для заданих значень інтенсивності створення блоків чесними майнерами α_H та зловмисними майнерами α_M, а також заданого часу синхронізації D_H, обчислити залежність ймовірності, що гілка, створена зловмисниками, стане довшою за гілку чесних майнерів, якщо в момент розгалуження гілка чесних майнерів була довшою на n блоків, від значення n. Побудувати відповідну таблицю розрахунків та графік залежності ймовірності в залежності від значення n.

Завдання 3. Розрахувати мінімальну кількість блоків підтвердження, які гарантують, що імовірність успішної атаки подвійної витрати буде не більшою ніж 10^{-3}.

Для заданого фіксованого значення інтенсивності створення блоків α необхідно написати програму, яка обчислить значення мінімальної кількості блоків підтвердження, що гарантують ймовірнісність успішної атаки подвійної витрати на рівні не більше ніж 10^{-3}. При цьому розрахунки необхідно провести в залежності від часу синхронізації D_H (яке приймає значення з відрізка $[0; 180]$) для різних значень хешрейту зловмисника: для $p_M = 0.15$, $p_M = 0.25$ і $p_M = 0.4$. Для кожного з трьох значень хешрейту зловмисника побудувати відповідну таблицю розрахунків та графік залежності мінімальної кількості блоків підтвердження в залежності від часу синхронізації.

Навести теоретичний опис проведених обчислень з відповідним обгрунтуванням.

5. Варіанти завдань:

1. $\alpha_H = 0.0009, \alpha_M = 0.0003, D_H = 60$ сек (для завдань 1 і 2); $\alpha = \alpha_M + \alpha_H$ (для завдання 3);
2. $\alpha_H = 0.0008, \alpha_M = 0.0004, D_H = 45$ сек (для завдань 1 і 2); $\alpha = \alpha_M + \alpha_H$ (для завдання 3);
3. $\alpha_H = 0.00075$, $\alpha_M = 0.0004$, $D_H = 30$ сек (для завдань 1 і 2); $\alpha = \alpha_M + \alpha_H$ (для завдання 3);

4. $\alpha_H = 0.0009, \alpha_M = 0.0004, D_H = 40$ сек (для завдань 1 і 2); $\alpha = \alpha_M + \alpha_H$ (для завдання 3);
5. $\alpha_H = 0.0008, \alpha_M = 0.0003, D_H = 30$ сек (для завдань 1 і 2); $\alpha = \alpha_M + \alpha_H$ (для завдання 3);
6. $\alpha_H = 0.0008, \alpha_M = 0.0005, D_H = 60$ сек (для завдань 1 і 2); $\alpha = \alpha_M + \alpha_H$ (для завдання 3);
7. $\alpha_H = 0.00085$, $\alpha_M = 0.00045$, $D_H = 45$ сек (для завдань 1 і 2); $\alpha = \alpha_M + \alpha_H$ (для завдання 3);
8. $\alpha_H = 0.00075$, $\alpha_M = 0.00035$, $D_H = 45$ сек (для завдань 1 і 2); $\alpha = \alpha_M + \alpha_H$ (для завдання 3);
9. $\alpha_H = 0.0009$, $\alpha_M = 0.00035$, $D_H = 60$ сек (для завдань 1 і 2); $\alpha = \alpha_M + \alpha_H$ (для завдання 3);
10. $\alpha_H = 0.00095$, $\alpha_M = 0.00055$, $D_H = 30$ сек (для завдань 1 і 2); $\alpha = \alpha_M + \alpha_H$ (для завдання 3).

6. Оформлення результатів роботи та звіту

Результатом роботи є всі тексти програм, скомпільовані виконувані файли (які мають запускатися на чистій ОС; якщо є потреба, можна використовувати контейнери), необхідна документація щодо використання програми з прикладами застосування та звіт.

Звіт до комп'ютерного практикуму оформлюється згідно зі стандартними правилами оформлення наукових робіт, за такими винятками:

- дозволяється використовувати шрифт Times New Roman 12pt та одинарний інтервал між рядками;
- дозволяється не починати нові розділи з окремої сторінки;
- дозволяється не включати анотацію, перелік термінів та позначень і перелік використаних джерел;
- не обов'язково оформлювати зміст.

Звіт має містити:

- мету проведення комп'ютерного практикуму;
- постановку задачі;
- хід виконання роботи, опис труднощів, що виникали, та шляхів їх подолання;
- теоретичне обґрунтування обчислень;
- таблиці з прикладами необхідних обчислень та графіки відповідних залежностей;
- детальний опис особливостей реалізації та приклади застосування;
- висновки до роботи.

Тексти програм не включати у звіт.

Комп'ютерний практикум вважається повністю виконаним після надіслання всіх текстів програм, скомпільованих виконуваних файлів, необхідної документації щодо використання програм з прикладами застосування, звіту.

7. Оцінювання комп'ютерного практикуму

За виконання комп'ютерного практикуму студент може одержати до 25 рейтингових балів; зокрема, оцінюються такі позиції:

- реалізація програми — до 10 балів;
- оформлення звіту — до 5 балів;
- теоретичне обґрунтування обчислень — до 10 балів;