Савин Ю. В., ассистент (УкрГУЖТ)

УДК 004.02: 519.1: 004.75

ПАРАЛЛЕЛЬНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА ДЕЙКСТРЫ. ЕГО ПРИМЕНЕНИЕ ДЛЯ РЕШЕНИЯ ЗАДАЧ ЛОГИСТИКИ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ

Вступление. В докладе рассматриваются вопросы оптимизации алгоритма Дейкстры для нахождения кратчайшего пути от одной вершины до всех остальных. Предлагаются варианты по инициализации данных и параллельной реализации самого метода. Применении алгоритма Дейкстры для оптимизации транспортного потока и улучшения логистики перевозок.

Презентация материала. Проблема оптимизации различного рода затрат при железнодорожных перевозках является актуальной. Методы теории графов позволяют успешно решать многие задачи логистики. Удобное и наглядное представление транспортной инфраструктуры в виде различных моделей графов позволяют легко формализовать задачу и найти её решение.

Алгоритм Дейкстры[1][2] для нахождения кратчайшего пути от одной вершины применим к различного рода графам: полносвязным и не полносвязным, ориентированным и не ориентированным и т.д. Ограничения, накладываемые на граф: он должен быть взвешенным и в нем должны отсутствовать ребра с отрицательными весами, идеально подходит для решения задач логистики на транспорте. Весами ребер могут выступать, в зависимости от конкретных условий, различные параметры оптимизации, например: время доставки груза, стоимость перевозки, качество железнодорожного полотна и т.д. Не смотря на отсутствие возможности условного прерывания работы алгоритма, он считается одним из наиболее быстрых алгоритмов в своей области. В классическом виде временная время сложность работы алгоритма $O(n^2)$.

В связи с активным ростом мощностей современных вычислительных систем за счет увеличения количества ядер в процессорах и применения специализированных ускорителей (графические ускорители, гибридные процессоры), интерес к возможности увеличения скорости работы алгоритма Дейкстры в параллельном режиме значительно возрос[3][4].

Вывод. В докладе представлены новые подходы к оптимизации алгоритма Дейкстры, и показаны возможности применения данного алгоритма для решения задач логистики на железнодорожном транспорте**.**

Список використаних джерел

1. A note on two problems in connexion with graphs, E. W. Dijkstra Numerische Mathematik, vol. 1, pp. 269–271, 1959. Available: http://dx.doi.org/10.1007/BF01386390
2. Жадные методы: Алгоритм Дейкстры // Алгоритмы. Введение в разработку и анализ Левитин А.В. — М.: Вильямс, 2006. — С.189–195. 576 с. — ISBN 978-5-8459-987-9
3. Monitoring distributed computing systems on the basis of the determined shortest paths and shortest hamiltonian cycles in a graph./ S. Listrovoy, S. Minukhin., E. Listrovaya // EasternEuropean Journal of Enterprise Technologies. – 2015. – Vol. 6, № 4 (78). – P. 32 – 45. DOI: 10.15587/1729-4061.2015.56247
4. A New GPU-based Approach to the Shortest Path Problem. H. Ortega-Arranz,Yu. Torres, D. R. Llanos ; A. Gonzalez-Escribano 2013 International Conference on High Performance Computing & Simulation (HPCS) DOI: 10.1109/HPCSim.2013.6641461

Сєвєрінов О. В., к.т.н. доцент,
Холоша О. С., бакалавр (ХНУРЕ)

АНАЛІЗ ЗАГРОЗ ВЕБ-ДОДАТКІВ

Кількість компаній та підприємців, які застосовують веб-технології для автоматизації процесів та поширення ринку збуту, постійно зростає. Наряду з перевагами користування веб-сервісами водночас приводить до підвищення рівня кіберзагроз інформаційній системі компанії. Зазвичай причиною більшості зломів є написаний розробником програмний код. Розробник може залишати вразливості в захисті програмного продукту, підчас просто не помітивши потенціальну вразливість.

Проведений аналіз дозволяє виділити основні види загроз [1, 2].

1. Виконання шкідливого коду. на сервері мережі. Якщо не дотримуватися вимог безпеки при розробці, то зловмисник може модифікувати хід виконання команд.

2. Атаки, що скеровані на методи ідентифікації та авторизації користувача, або на методи, які використовуються веб-сервером для визначення того, чи має користувач необхідні повноваження для подальшого користування веб-ресурсом.

3. Атаки на клієнтів. Під час використання веб-додатку, між користувачем і сервером встановлюються довірчі відносини. Використовуючи цю довіру, зловмисник може використати різні методи для проведення атак на клієнтів сервера.

4. Витік або розголошення критичної інформації безпосередньо про сайт, його компоненти, платформу і складові, так і витік конфіденційної інформації з сайту, через її неналежний захист. Це розкриття інформації,

доступ до якої заборонено, або розкриття інформації в результаті невірного налаштування сайту або веб-сервера.

5. Логічні атаки спрямовані на експлуатацію функціоналу сайту. Додаток може вимагати від користувача коректного виконання кількох послідовних дій для виконання певного завдання. Зловмисник може обійти або використовувати ці механізми у своїх цілях.

Таким чином, при розробці веб-додатку необхідно планувати його архітектуру таким чином, щоб уникнути можливих ризиків та загроз.

Список використаних джерел

1. Сєвєрінов О.В. Аналіз сучасних методів атак на електронні ресурси органів управління / О.В. Сєвєрінов, В.О. Шевцов, А.С. Сокол-Кутиловська // Системи озброєння і військова техніка. – Х: ХНУПС. - 2017. – Вип. 1(49). – С. 65-68.
2. Бирюков А.А. Информационная безопасность: защита и нападение. – М.: ДМК Пресс, 2012. – 474 с.

Сєвєрінов О. В., к.т.н. доцент,
Щербина Д. В., студент (ХНУРЕ)

АНАЛІЗ МОЖЛИВОСТІ ВИКОРИСТАННЯ ПОРОГОВИХ ПІДПИСІВ

У даний час в системах управління критичної інфраструктури все більше уваги приділяють проблемам захисту інформації. Одним з питань при цьому є використання порогових підписів. Тому актуальних питанням є проведення аналізу алгоритмів порогового підпису, їх порівняння з іншими схемами групових підписів та можливості практичного використання у інформаційних системах.

Схема підпису k з n – це протокол, який дозволяє будь-якій підмножині k гравців з n генерувати загальний підпис, але це виключає створення дійсного підпису, якщо в протоколі бере участь менше, ніж k гравців [1].

Проведенний аналіз показав, що практичне застосування групових підписів (підпис k з n) стримується широким колом їх недоліків:

1. відсутність жорстких доказів безпеки навіть у випадковій моделі оракулів;

2. генерація та (або) верифікація частки підпису є інтерактивною, крім того, вимагає синхронної мережі зв'язку;

3. розмір окремої частки підпису лінійно збільшується зі збільшенням кількості гравців.

Вирішення цих недоліків можливе при використанні порогових підписів. Пороговий підпис – це простий криптографічний метод генерації розподіленого ключа і підпису до нього, який має властивості [1]:

1. виключення можливості підробки часткового секрету, який по своїй суті є підписом;

2. створення та перевірка частки підписів повністю неінтерактивні;

3. розмір окремої частки підпису обмежений невеликим постійним значенням.

Ще одним недоліком схем розділення секрету є їх принципово одноразове використання, оскільки при реконструкції загального секрету, сам секрет стає відомим усім учасникам, що його відновлювали. Порогова криптографія дозволяє здійснювати більш багаторазовий підхід – згідно з яким достатній кворум учасників може погодитися використовувати секрет для виконання криптографічних обчислень, не обов'язково реконструюючи секрет у процесі.

Основна властивість порогових підписів полягає в тому, що приватний ключ ніколи не потрібно реконструювати. Навіть після багаторазового підписання ніхто не дізнається жодної інформації про приватний ключ, який дозволив би кожному окремо підписувати рішення без групування [2].

Проведений аналіз показав, що порогові підписи є більш гнучкими, порівнюючи з мультипідписами, у можливості змінювати політику доступу. Їх використання дозволяє застосувати багатосинхронну політику контролю доступу у здійсненні та завіренні деякого спільного рішення, що врешті буде публічно розголошено.

На практиці порогові підписи використовуються в блокчейн-клієнтах (наборах команд виконуваних повною нодою) для зміни процесу генерації створення ключів і підписів. Застосування саме даного підходу дозволяє вносити зміни для всіх команд, пов'язаних з розподіленими обчисленнями і приватним ключем.

Децентралізовані додатки, рішення масштабованості другого рівня, атомарні свопи, мікшування, успадкування та інші функції, які можуть бути реалізовані в рамках блокчейн технології все частіше заміняються криптографією на основі порогових підписів. Це дозволяє замінити дорогі і ризиковані всередині ланцюгові операції зі смарт-контрактами на більш дешеву і надійну альтернативу.

Таким чином, схеми порогових підписів є більш гнучкими та менш громіздкими, порівнюючи зі схемами підпису k з n.

В даний час порогові підписи активно використовуються у блокчейн-клієнтах, як потужний аналог мультипідписів, та у різноманітних корпоративних бізнес рішеннях.

Список використаних джерел

1. A. Boldyreva, «Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme,» in Public key cryptography – PKC