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,