УДК 004.056.52

А.М. Давиденко, Київ
О.А. Суліма, Київ
О.А. Давиденко, Київ

ВИКОРИСТАННЯ ДВОРІВНЕВОЇ МОДЕЛІ ДОСТУПУ ДО ДАНИХ ДЛЯ ВИРІШЕНЯ ПРИКЛАДНОЇ ЗАДАЧІ З ПРОВЕДЕННЯ ОБ'ЄКТУ ПО ТЕРИТОРІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Abstract. We propose example of building an empowerment system for the use of confidential data contained in the information system. The empowerment system is an important component of the information system access security system. Therefore, the paper examines the methods of building a system for granting authority that provides a certain level of security access to confidential data, which are closely related to the degree of confidentiality of relevant data contained in the information system.

Актуальність

В роботах [1 – 2] обґрунтовано актуальність, поставлено та розв'язано задачу реалізації системи надання повноважень, яка ґрунтується на використанні дворівневої моделі надання повноважень. Оскільки дані, що знаходяться в інформаційній системі, потрібні для розв'язання прикладних задач, то на першому рівні розглядається задача надання доступу до системи користувачу, який повинен розв'язати прикладну задачу. На другому рівні система надає повноваження прикладній задачі, якій для розв'язання, крім інших даних, потрібні конфіденційні дані з певним рівнем конфіденційності. Задача надання повноважень прикладним задачам розв'язується на підставі аналізу параметрів задачі, і при цьому не приймаються до уваги параметри користувача.

Постановка задачі

Використання дворівневої моделі доступу до даних дозволяє створити програмне забезпечення, яке за певних умов може отримати доступ до інформації більш високого рівня доступу, не розголошуючи її змісту.

Якщо прийняти, що предметом експерименту є система доступу, об'єкти – прикладні задачі, рух об'єкту – процес розв'язання прикладної задачі, Траєкторія руху об'єкту – алгоритм розв'язання задачі, пункт, що зустрічається на траєкторії руху – дані, які потрібні для продовження процесу розв'язання, засоби управління доступом до пунктів, що зустрічаються на траєкторії руху на вході до пункту – система доступу, яка визначає чи відповідні дані можна надати об'єкту, траєкторія проходить через пункт – система надала дані задачі, траєкторія руху об'єкту обходить пункт – система надала дані результатів розв'язання фрагменту задачі, які отримала в результаті використання

дозволених алгоритмів перетворення відповідних даних, траєкторія руху об'єкту обходить пункт та модифікує наступні фрагменти траєкторії у відповідності з наданими рекомендаціями системи надання повноважень – система надала дані результатів розв'язання фрагменту задачі, які отримані використанням алгоритмів, що реалізують допустимі для відповідних даних перетворення та отримані результати перетворила в дискретні величини, на основі яких реалізується модифікація наступного фрагменту процесу розв'язання, траєкторія руху об'єкту модифікується з урахуванням рекомендацій системи по модифікації цілі розв'язання задачі – система надала дані розв'язання фрагменту задачі, які отримала використовуючи свій алгоритм їх перетворень та на основі отриманих результатів система формує рекомендації по модифікації цілі, що є необхідним для успішного продовження процесу розв'язування задачі, то не розкриваючи повністю предметну область інтерпретації, а обмежившись лише критичними умовами її реалізації розглянемо наступну прикладну задачу.

Нехай задано три суміжні області *A, B, C.* Причому області *A* і *C* не мають спільних кордонів і шлях з *A* в *C* пролягає через *B*. У області *B* розташовано деякі об'єкти, інформація про які є конфіденційною. Нам необхідно провести об'єкт з області *A* в область *C*. При цьому не розголошуючи конфіденційної інформації з області *B*. Класична модель доступу вирішує цю проблему за рахунок обходу області *B* межею. Використовуючи дворівневу модель доступу до даних, можна побудувати критерій не розголошення конфіденційної інформації. Наприклад, дозволити рух об'єкта в області *B* та, аналізуючи траєкторію його руху, з метою не допущення його попадання у деяку область контакту об'єктів з області *B*. За рахунок цього буде відбуватися скорочення проходження шляху об'єкта. Слід зауважити, що існує деяка мінімальна відстань, менше якої скоротити шлях неможливо. Проведемо серії експериментів, генеруючи в області *B* чотири об'єкти, випадковим чином дотримуючись рівномірного розподілу (завдання контролю об'єкта, забороненої території і території обмеженого доступу), для об'єкта з області *A* будується гарантований обхідний маршрут і будується маршрут проходження через область *B* з деякою точністю *H*. Критерієм не розголошення встановимо не допущення наближення об'єкта з області *A* до об'єктів з області *B* на відстань *D*. Алгоритм пошуку шляху у таких умовах працює не отримуючи інформації про розташування об'єктів області *B*, що відповідає нашим вимогам з конфіденційності. Результатом експерименту буде розрахунок довжини скороченого шляху у частках від максимального (обхідного) шляху.

Вирішення задачі

Для реалізації програмного забезпечення було обрано мову програмування Python 2.7. Загальна назва розробленого програмного пакета «Security Visualizer». Даний пакет складається з наступних програмних модулів: «matrixmodel.exe» – меню, яке дозволяє обрати параметри запуску

для «visualizer.exe»; «visualizer.exe» – програма, яка відображає карту з точками, до яких має доступ користувач. Вона приймає від «matrixmodel.exe» або командного рядка два аргументи – рівень і колір доступу користувача та читає точки з файлів «red.csv», «green.csv», «blue.csv», «yellow.csv». Зазначені файли необхідні для вивчення і демонстрації матричної моделі доступу. Друга група файлів, яка входить до програмного пакету «Security Visualizer» реалізує модель пошуку шляху. Це «pathfindermodel.exe» – меню, яке дозволяє вибрати параметри запуску для pathfinder.exe; «pathfinder.exe» – програма, яка знаходить на карті між двома заданими точками наближено найкоротший маршрут, який обминає кожну з чотирьох точок, які випадково згенеровано у просторі між початковою і кінцевою точками. Відображає усі точки, знайдений маршрут і окремий обхідний маршрут, який складається з двох відрізків і гарантовано обминає згенеровані точки. Програма «pathfinder.exe» приймає від «pathfindermodel.exe» або командного рядка два обов'язкові аргументи: радіус наближення (мінімальна відстань, на яку може наблизитися маршрут до точки) і точність розрахунку маршруту. Також у режимі командного рядка може приймати третій аргумент – кількість експериментів. Зазначена програма здійснює експеримент (генерація набору з чотирьох точок і пошук найкоротшого маршруту). Для кожного експерименту запам'ятовується довжина знайденого маршруту як відсоток від довжини обхідного маршруту. Ця інформація записуються у файл «result.csv». Початкова і кінцева точки читаються з файлів «start.csv» і «end.csv» відповідно. Всі програмні модулі використовують вхідні дані з папки «data». Алгоритм пошуку засновано на відомому алгоритмі Лі з метою здійснення виявлення найкоротшого шляху на основі графів з ребрами одиничної довжини. Цей алгоритм належить до групи алгоритмів пошуку в ширину та призначений для визначення найбільш короткого шляху. Його цільове призначення є знаходження довжини.

Таким чином, для проведення експерименту необхідно запустити «pathfindermodel.exe». У меню (рис. 1) задати параметри моделювання і відкрити карту (рис. 2).

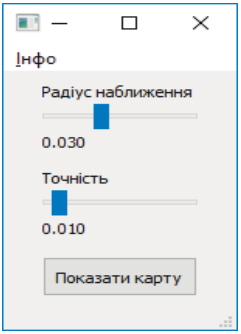

Рис. 1. Меню вибору параметрів

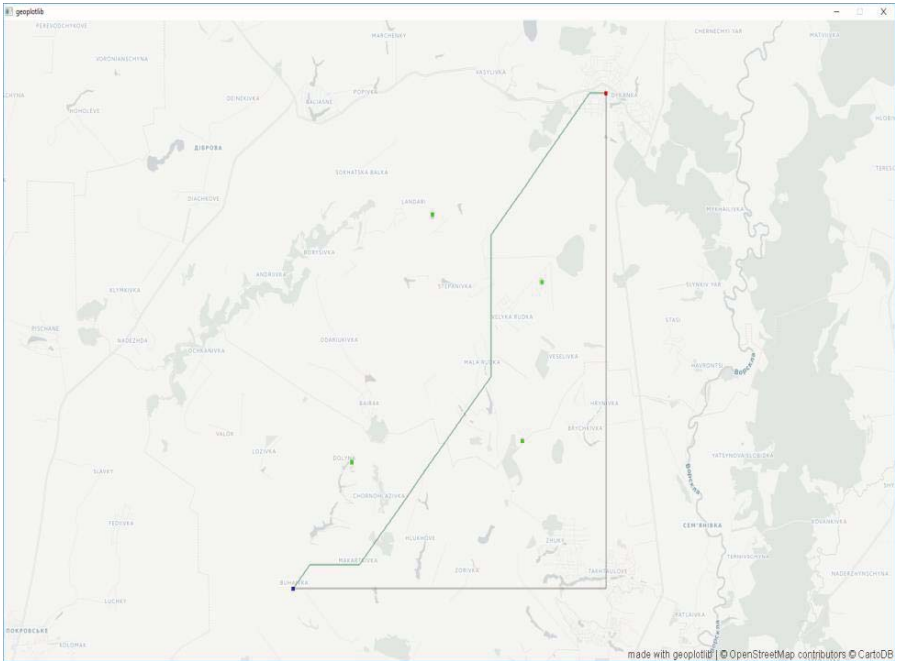

Рис. 2. Результати одиничного розрахунку

На карті видно обхідний маршрут (горизонтальна і вертикальна прямі), синя і червона точки – початок і кінець маршруту, зелені точки – доступ, до яких заборонено, і ламана крива лінія показує маршрут, який розроблено з використанням дворівневої моделі доступу до даних.

Для оцінки користі від застосування дворівневої моделі доступу до даних у даній прикладної задачі проведемо 1000 експериментів, результати яких наведено на рис. 3. По осі Y показано кількість точок, що потрапляють в інтервал, який аналізується; по осі X – частка від максимального шляху. Математичне сподівання частки шляху становить 0,8025. Тобто середній виграш від застосування дворівневої моделі доступу до даних, при 1000 експериментах становить 19,75% від максимального шляху.

Характер кривої нагадує нормальний розподіл. Для уточнення побудуємо поверхню, яка показує результати більшого числа експериментів. У таблиці наведено розподіл кількості результатів при фіксованих D і H для різного числа експериментів.

На рис. 4 приведено графічні результати проведених експериментів при зростанні їх числа.

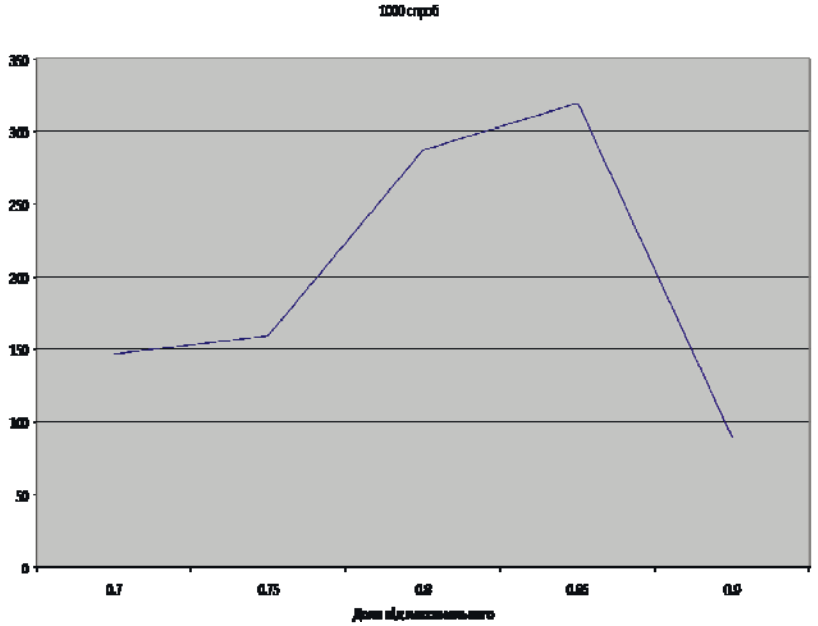

Рис. 3. Результати тисячі експериментів

Таблиця

Розподіл кількості результатів для різного числа експериментів

Радіус наближення D	Точність розрахунку H	Кількість точок в інтервалі X±0.025					Число експериментів
		0.7	0.75	0.8	0.85	0.9	
0.03	0.01	146	159	287	319	89	1000
0.03	0.01	242	357	561	653	187	2000
0.03	0.01	345	510	842	980	323	3000
0.03	0.01	461	670	1120	1319	430	4000
0.03	0.01	610	925	1300	1655	510	5000
0.03	0.01	745	1075	1685	1865	630	6000
0.03	0.01	831	1235	1959	2245	730	7000
0.03	0.01	971	1435	2175	2509	910	8000
0.03	0.01	1123	1610	2400	2797	1070	9000
0.03	0.01	1250	1800	2720	3133	1097	10000

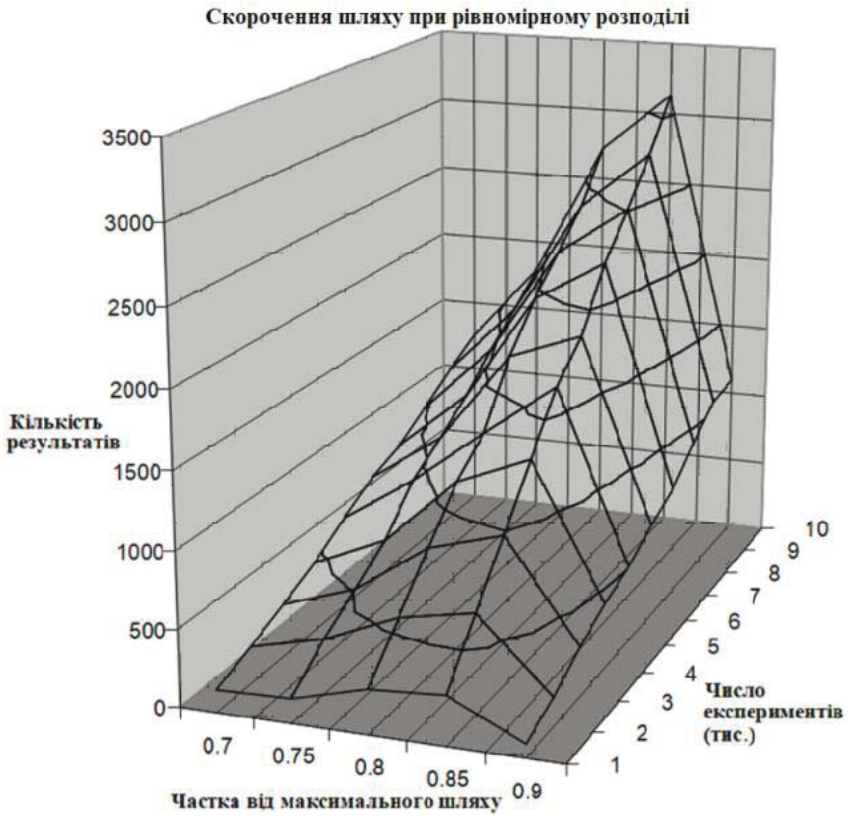

Рис. 4. Результати експериментальних досліджень

Висновки Аналізуючи отриману поверхню видно, що із збільшенням кількості проведених експериментів форма кривої наближається до класичної для нормального розподілу. Математичне сподівання частки шляху становить 0,8113 тобто середній виграш від застосування дворівневої моделі при 10000 експериментах становить майже 19% від максимального шляху.

1. *Давиденко А.М., Суліма О.А.* Використання формальних засобів опису процесів надання повноважень // Захист інформації. – К. 2016. Т. 18, № 2. – С.143-149.
2. *Суліма О.А.* Модель багаторівневої системи доступу // Безпека інформації. – К. 2017. – Т. 23, № 2. – С.123-130.

Поступила 12.10.2017р.