



2. Кириллов Д.В. Классификация моделей делегирования полномочий в контроле доступа на основе ролей// Доклады Томского государственного университета систем управления и радиоэлектроники, 2010, № 1(21), с. 146-150.
3. Кириллов Д.В. Особенности механизма обработки событий в СОДОП//Материалы Зимней школы аспирантов и молодых ученых УГАТУ, Уфа, 2009.
4. Ahmed Ali, Zhang Ning A Context-Risk-Aware Access Control Model for Ubiquitous Environments // Proceedings of the International Multiconference on Computer Science and Informational Technologies. - Wisla, Poland :, 2008. - стр. 775-782.
5. Al-Kahtani Mahammad A. A model for Attribute-Based User-Role Assignment // Proceedings of the 18th Annual Computer Security Applications Conference. - Washington, DC, USA : IEEE Computer Society, 2002.
6. Kumar A.N., Karnik N. и Chaffle G. Context sensitivity in Role-Based Access // ACM SIGOPS Operating system review. - July 2002 r. - Т. 36. - стр. 53-66.
7. Кириллов Д.В. Классификация моделей делегирования полномочий в контроле доступа на основе ролей// Доклады ТУСУРа, № 1 (21), часть 1, июнь 2010.стр.146-149.

К.Е. Климентьев

ГЕНЕРАЦИЯ СЛУЧАЙНЫХ ГРАФОВ С ТРЕБУЕМЫМИ СВОЙСТВАМИ

(Самарский государственный аэрокосмический университет имени академика С.П. Королева (национальный исследовательский университет))

Силами преподавателей и студентов факультета информатики СГАУ ведется работа над реализацией системы имитационного моделирования распространения и взаимодействия вредоносных программ в компьютерных сетях. Одной из задач при этом является имитация сетей с требуемой топологией и статистическими характеристиками [1]. Класс сетей, служащих для моделирования среды существования «мобильных» червей, носит наименование «специального» («ad hoc») и представляет собой подмножество случайных графов [2]. Наиболее близкими абстракциями для подобных сетей являются случайный граф Радо (он же граф Эрдеша-Реньи) и «геометрический» случайный граф. Они различаются методами построения.

Случайный граф Радо (RRG) получается из «полного» графа, каждое ребро которого остается с заранее выбранной вероятностью p и удаляется с вероятностью $1-p$. Степени k_i всех вершин в таком графе примерно одинаковы, более точно - их количество подчиняется биномиальному распределению $P(k_i = k) = NC_{N-1}^k p^k (1-p)^{N-1-k}$ со средней степенью вершины $\bar{k} = p \times N$, где N - количество вершин [2].

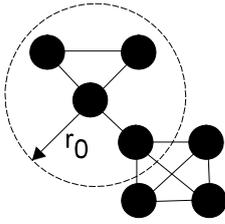


Рис. 1. «Геометрический» случайный граф

Граф со случайной геометрией строится на множестве вершин, случайно и равномерно распределенных в единичном квадрате. Ребро между двумя вершинами (x_i, y_i) и (x_j, y_j) проводится в том случае, если расстояние между ними $r = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \leq r_0$, где r_0 - заранее оговоренный «радиус действия».

Для получения желаемых статистических свойств «геометрического» графа необходимо изучить распределение величины r . Более общая задача решена, например в [4], однако там отсутствует выражение для функции распределения $F(r)$.

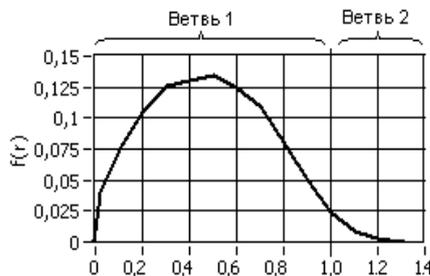
С помощью известных соотношений теории вероятностей [3] самостоятельно получены следующие результаты.

Распределение расстояний между двумя случайными точками единичного квадрата состоит из двух «ветвей» (см. рис. 2). Практически всегда в единичном квадрате расстояние $r < 1$ и подчиняется закону с плотностью

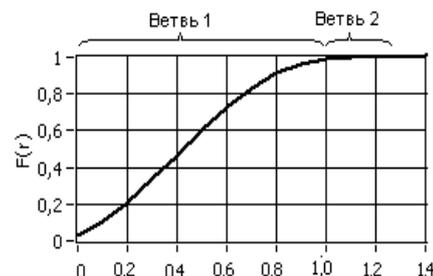
$$f(r) = 2r^3 - 8r^2 + 2\pi r$$

и функцией распределения

$$F(r) = 0.5r^4 - \frac{2}{3}r^3 + \pi r^2.$$



а) Плотность распределения $f(r)$



б) Функция распределения $F(r)$

Рис 2. Распределение расстояния между двумя случайными точками

В остальных, гораздо более редких случаях $1 \leq r \leq \sqrt{2}$:

$$f(r) = -2r^3 + 2r^2\sqrt{r^2 - 1} + r(4 - 2\pi - 8\arctan(\sqrt{r^2 - 1}));$$

$$F(r) = -\frac{1}{2}r^4 - 4r^2 \arctan(\sqrt{r^2 - 1}) + \frac{1}{3}(2r^2 + 1)\sqrt{r^2 - 1} + (\pi - 2)r^2 + \frac{1}{3}.$$

Математическое ожидание расстояния $m(r) = \frac{1}{15}(2 + \sqrt{2} + 5\arcsin(1)) \approx 0.52$. Очевидно,

средняя степень вершин соответствующего графа зависит от r_0 :

$$\bar{k} = N \times P(r < r_0) = N \times F(r_0).$$

В качестве примера применения полученных соотношений приведем результаты генерации случайных графов типов RRG и RGG с $N=30$ вершинами и ожидаемой средней степенью вершин $\bar{k} = 10$.



а) Граф типа RRG, $p=0.33$, $\bar{k} \approx 9.13$

а) Граф типа RGG, $r_0=0.39$, $\bar{k} \approx 9.46$

Рис. 3. Графы разных типов с одинаковой средней степенью вершин

Граф типа RGG обладает более регулярной структурой, граф RGG характеризуется наличием «малых миров» (сгущений). Эти особенности существенны при моделировании конкретных эпидемий сетевых червей.

Литература

1. Климентьев К.Е. Моделирование распространения и взаимодействия самовоспроизводящихся объектов [Текст] / К.Е. Климентьев // Известия Самарского научного центра РАН. - Самара: изд-во СНЦ РАН, 2014. – т.16 №4(2) - С. 313-317.
2. Райгородский А.М. Модели случайных графов и их применения [Текст]/ А.М. Райгородский // М.: Труды МФТИ. – 2010. – Том 2, №4. – С. 130-140.
3. Вентцель Е.С., Овчаров Л.А. Прикладные задачи теории вероятностей [Текст]/ Е.С. Вентцель [и др.]. – М.: Радио и связь, 1983. – 416 с.
4. Philip J. The probability distribution of the distance between two random points in a box [Текст]/ J. Philip // TRITA MAT 7(10), 2007. – 13 pp.

А.В. Козачок, Л.М. Туан

ОБОСНОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ НЕРАЗЛИЧИМОЙ ОБФУСКАЦИИ ДЛЯ ЗАЩИТЫ ИСПОЛНЯЕМЫХ ФАЙЛОВ

(Академия ФСО России)

В настоящее время угрозы информационной безопасности, связанные с утечкой конфиденциальных данных, являются одними из наиболее опасных для любой организации, так как приводят к прямым материальным убыткам и ущербу, потере интеллектуальной собственности. По мере развития компьютерных технологий и услуг связи растет число возможных каналов утечки информации.

Целью проводимого исследования является построение системы защиты исполняемых файлов от несанкционированного доступа. Для достижения поставленной цели был выбран подход на основе обфускации программного кода.