ПРИМЕНЕНИЕ НОВЫХ МЕТОДОВ ВИЗУАЛИЗАЦИИ ДЛЯ ОТОБРАЖЕНИЯ МЕТРИК БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СЕТИ

А. А. Чечулин, М.В. Коломеец, И.В. Котенко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича, Санкт-Петербургский институт информатики и автоматизации РАН

Санкт-Петербург, Россия

РусКрипто’2016, 22-25 марта 2016 г.

План доклада

- Введение
- Виды визуальных моделей
- Построение диаграммы Вороного
- Выводы

План доклада

- **Введение**
- Виды визуальных моделей
- Построение диаграммы Вороного
- Выводы

Введение

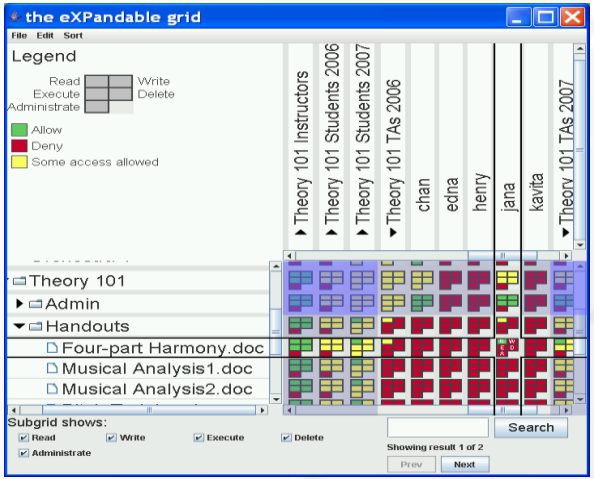
- Визуальная аналитика является эффективным инструментом для анализа данных
  - зрительная система является основным каналом передачи информации от компьютера к человеку
  - зрительное восприятие информации является мощным и точным механизмом поиска паттернов
  - визуализация помогает справиться с растущим объемом данных
  - методы визуальной аналитики могут применяться при работе с большими данными и для обеспечения ситуационной осведомленности в критических предметных областях
  - ситуационная осведомленность в области кибербезопасности призвана обеспечить получение ответов на вопросы, связанные с тем, что и почему происходит в сети, каково текущее воздействие атаки и каков возможный ущерб

План доклада

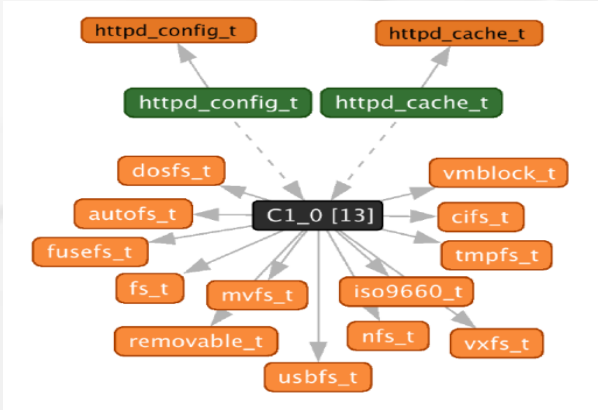
- Введение
- **Виды визуальных моделей**
- Построение диаграммы Вороного
- Выводы

Представление политик безопасности

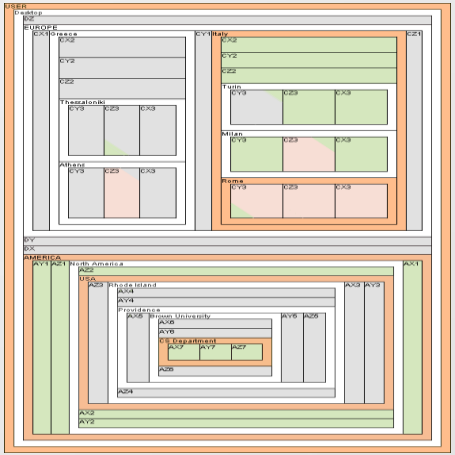
Матричное представление прав доступа к ресурсам [1]



Представление прав доступа к ресурсам в виде графа [2]



Представление прав доступа к ресурсам в виде карты деревьев [3]

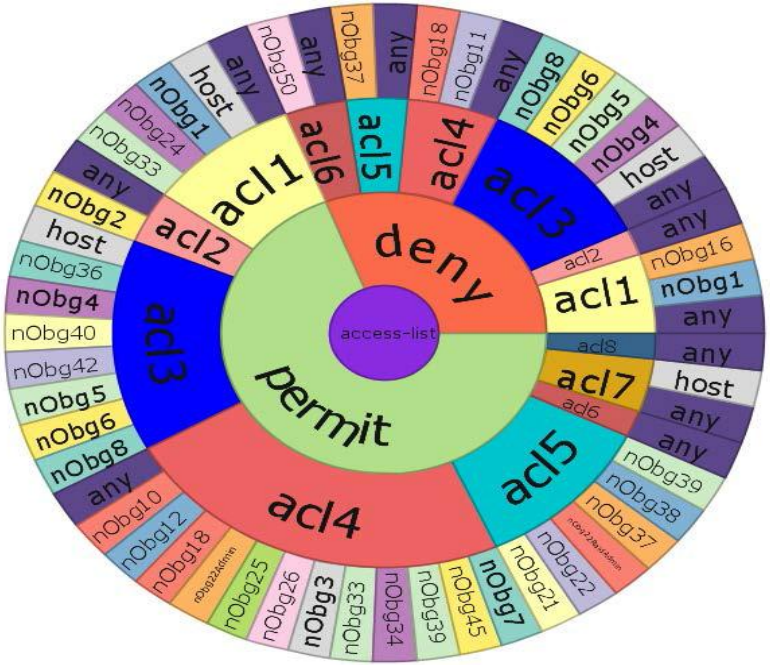


[1] Reeder R. W., Bauer L., Cranor L. F., et al. Expandable grids for visualizing and authoring computer security policies. *SIGCHI Conference on Human Factors in Computing Systems* (CHI '08). ACM, New York, NY, USA, 2008.

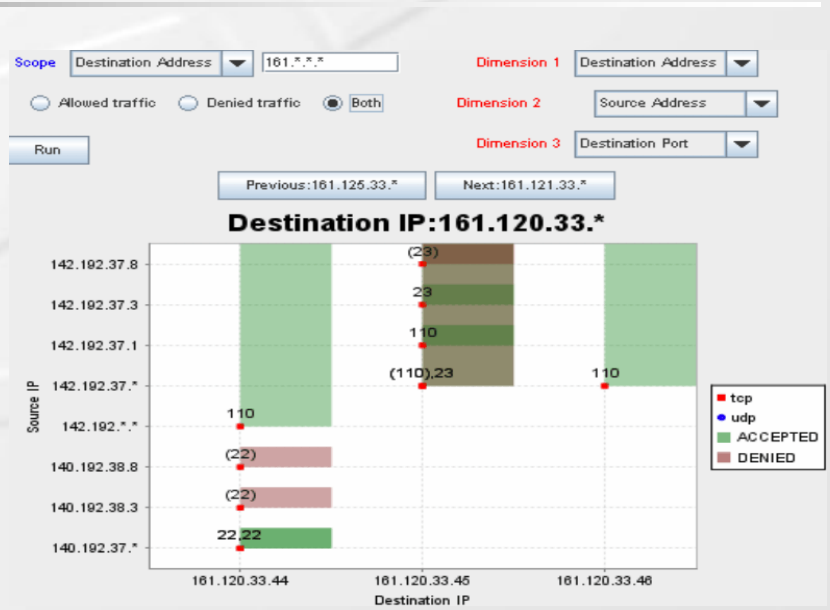
[2] Marouf S., Shehab M. SEGrapher: Visualization-based SELinux PolicyAnalysis. 4th Symposium on Configuration Analytics and Automation (SAFECONFIG), 2011.

[3] Heitzmann A., Palazzi B., Papamanthou C., Tamassia R. Effective Visualisation of File System Access-Control. 5th international workshop on Visualisation for Computer Security (VizSec'08), LNCS, Vol.5210, Springer-Verlag, Berlin, Heidelberg, 2008.

Представление правил межсетевых экранов



Визуализация в виде "солнечные лучи" (Sunburst) [1]

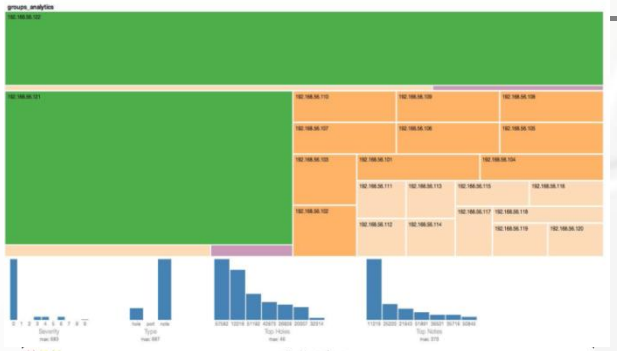


PolicyViz [2]

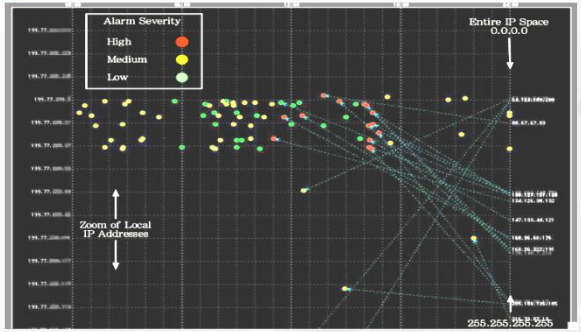
[1] Mansmann F., Göbel T., Cheswick W. Visual Analysis of Complex Firewall Configurations. VizSec'12, October 15, 2012, Seattle, WA, USA, 2012.

[2] Tran T., Al-Shaer E., Boutaba R. PolicyVis: Firewall Security Policy Visualisation and Inspection. 21st Conference on Large Installation System Administration Conference (LISA'07), USENIX Association, Berkeley, CA, USA, 2007.

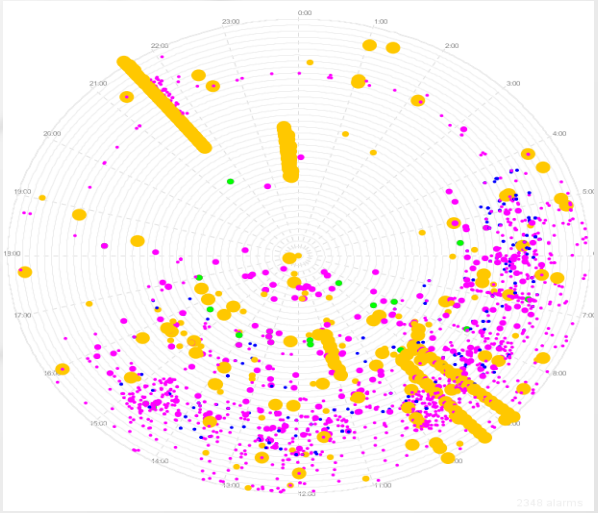
Представление уязвимостей и событий безопасности



Nv Tool [1]



IDS Rainstorm [2]



Спиральное представление событий безопасности [3]

[1] Harrison, L., Spahn, R., Iannacone, M., Downing, E., Goodall, J.R.: NV: Nessus Vulnerability Visualisation for the Web. Proc. of the VizSec'12, October 15 2012, Seattle, WA, USA (2012)
[2] Abdullah K., Lee C., et al. IDS Rainstorm: Visualizing ids alarms. IEEE Workshops on Visualization for Computer Security, 2005.
[3] Bertini E., Hertzog P., Lalanne D. SpiralView: Towards Security Policies Assessment through Visual Correlation of Network Resources with Evolution of Alarms. IEEE Symposium on Visual Analytics Science and Technology (VAST) 2007.

OSSIM: карта рисков

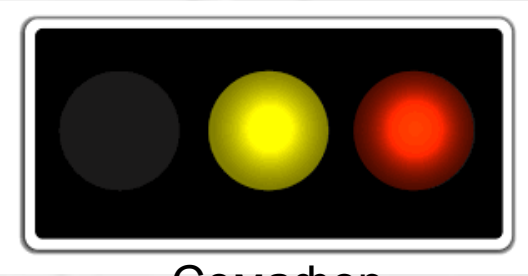
Карта рисков отображает информацию о состоянии риска (R), уязвимостей (V) и доступности (A) каждого сетевого объекта, расположенного на карте в виде светофоров

Виды визуальных моделей (1/3)

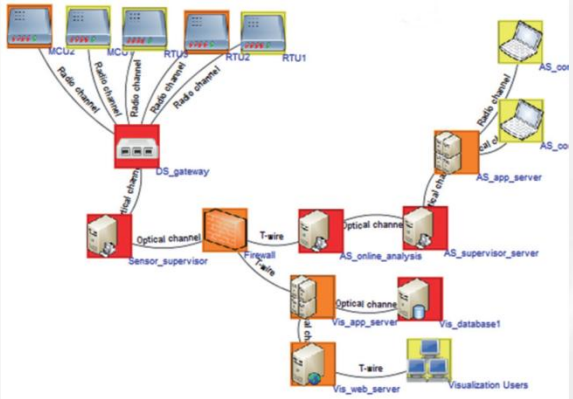
Информативность vs Понятность

Input Packet Length	Input Rate	Input Media Overhead (Ethernet)	Total Input Port bytes	MAC removed bytes (including CRC)	Other PP/MAC/FRAMER removed bytes	PP Packet add bytes (to fabric and peer PP)	Switch Port Packet Size	Switch Port effective Input Rate
64	1.00E+10	20	84	24	0	12	72	8.57E+09
128	1.00E+10	20	148	24	0	12	136	9.19E+09
256	1.00E+10	20	276	24	0	12	264	9.57E+09
1500	1.00E+10	20	1520	24	0	12	1508	9.92E+09

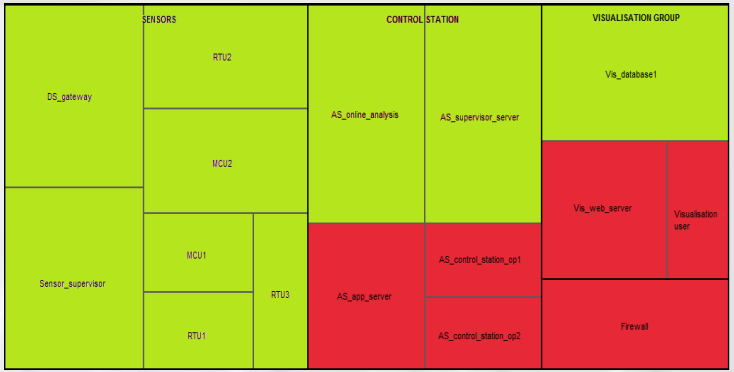
Таблица



Семафор



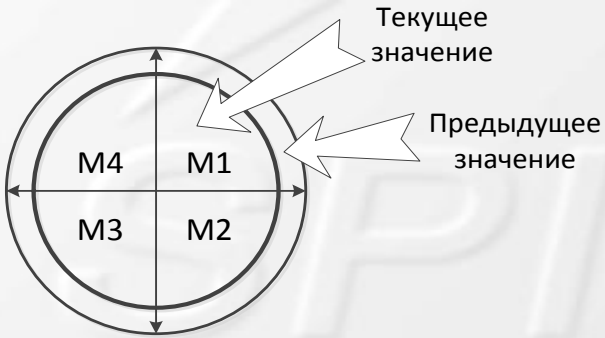
Граф компьютерной сети

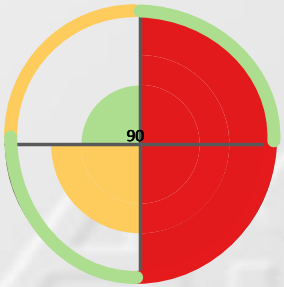


Карты деревьев

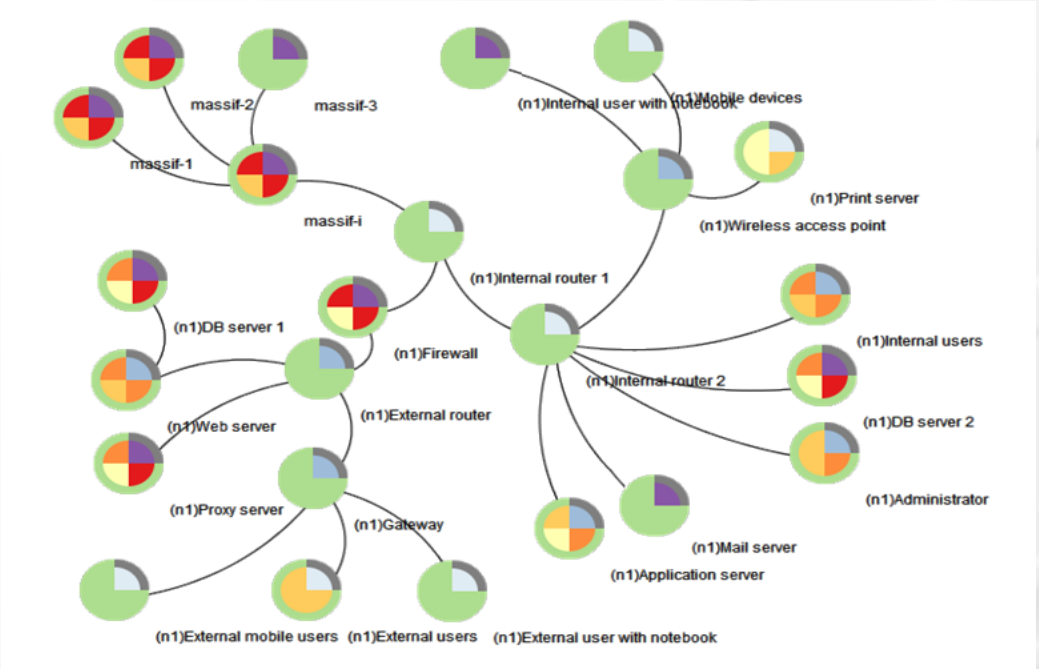
Виды визуальных моделей (2/3)

- Для предоставления пользователям возможности анализировать несколько метрик предложена модель визуализации (глиф) на основе кругов, способная отображать предыдущие значения метрик
- Круг разделяется на n секторов, которые отображают значения n метрик. Внешние кольца представляют предыдущие значения
- Для отображения критичности значения используется цвет
- Модификация этой модели – от критичности значения метрики зависит радиус сектора





Виды визуальных моделей (3/3)



Глифы

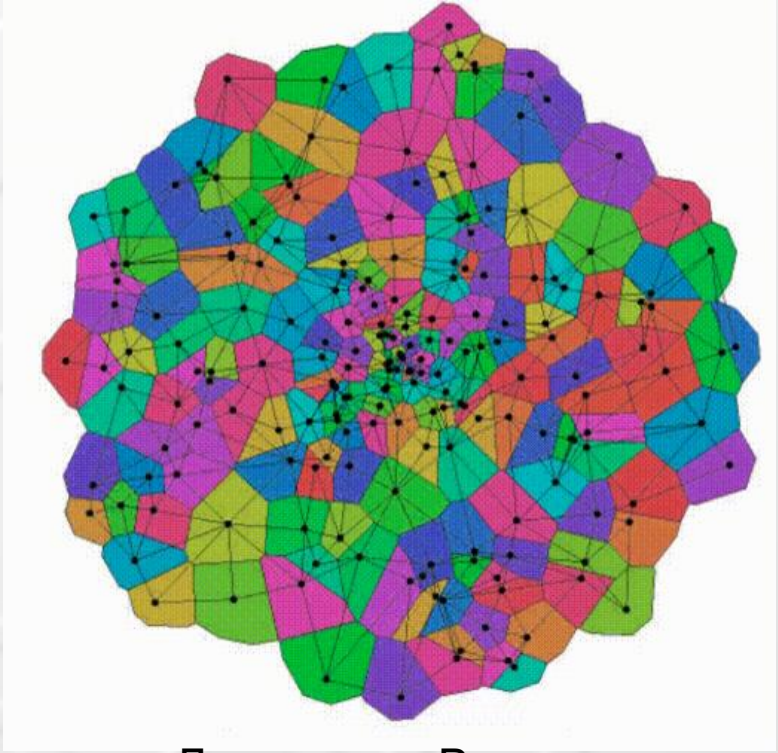


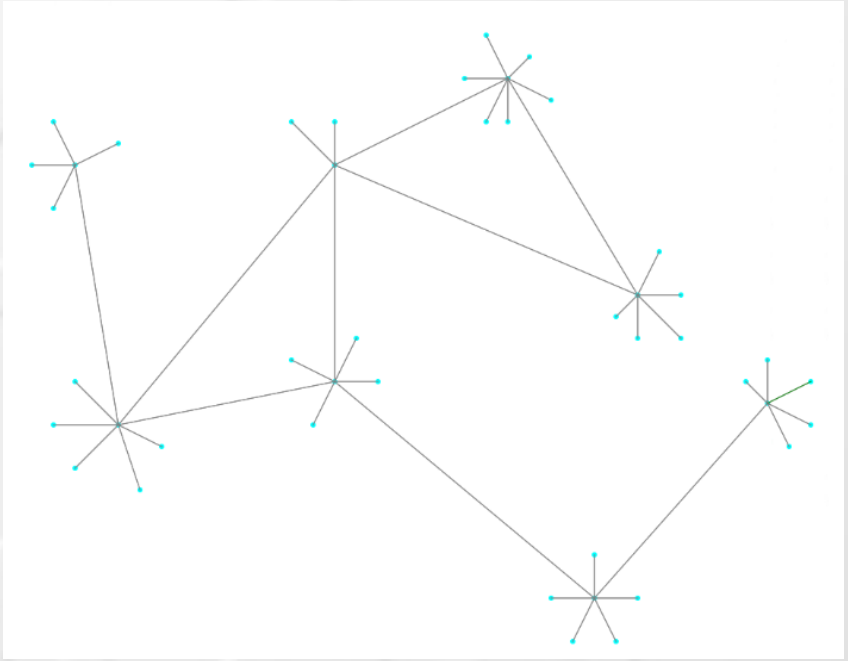
Диаграмма Вороного

План доклада

- Введение
- Виды визуальных моделей
- **Построение диаграммы Вороного**
- Выводы

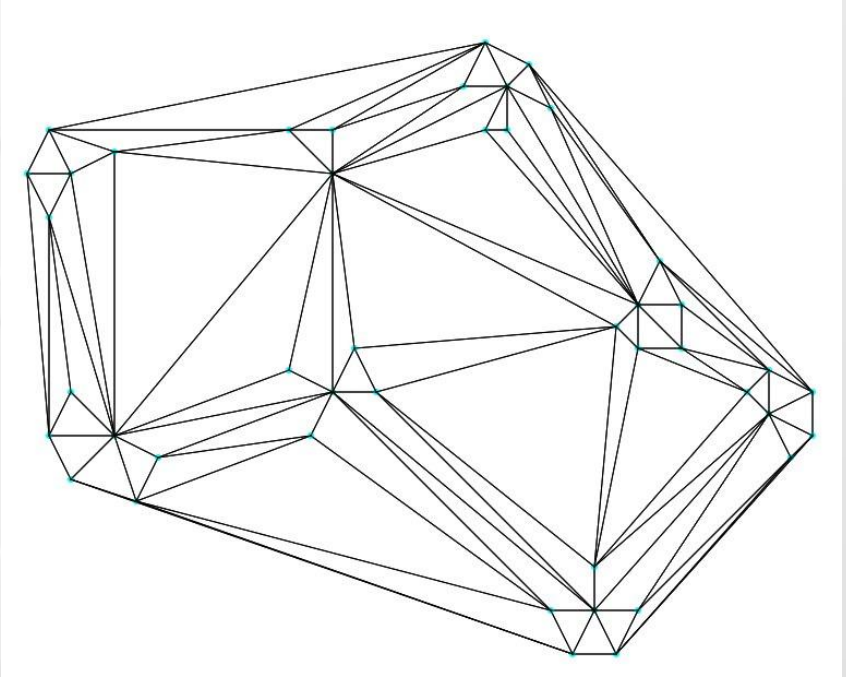
Построение диаграммы Вороного

Граф задаётся как список хостов, каждый из которых хранит поля-метрики хоста и список ссылок на хосты отношения.
Ограничение – граф должен быть планарным.



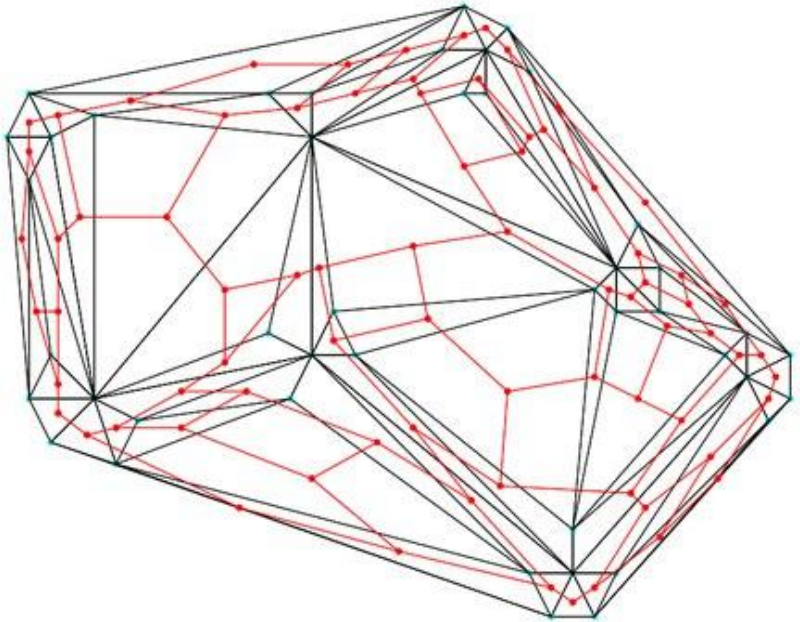
Построение диаграммы Вороного

Перед триангуляцией строится выпуклая оболочка.
Так как при триангуляции необходимо сохранить уже существующую структуру оболочки и графа, используется алгоритм ограниченной триангуляции Делоне.



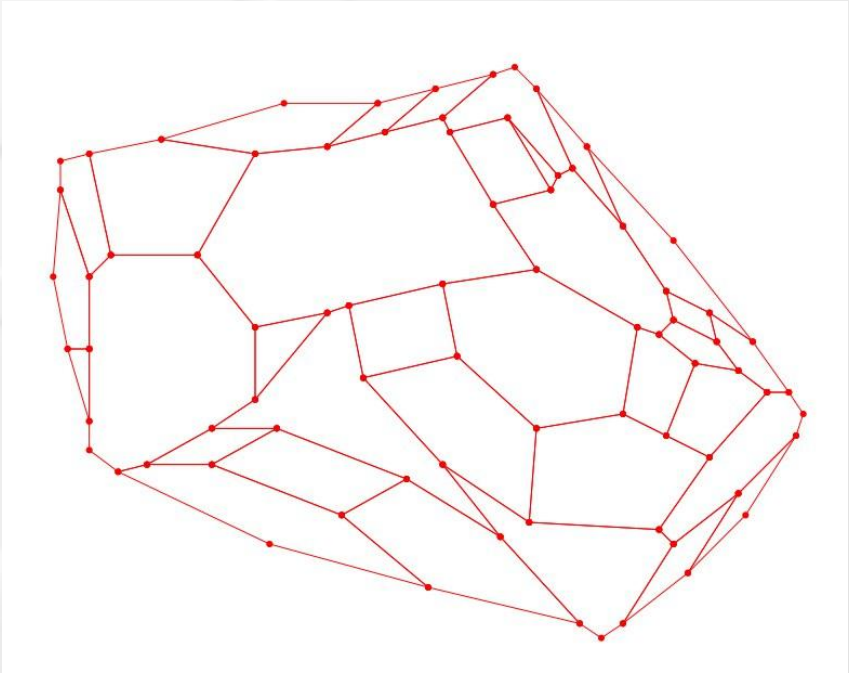
Построение диаграммы Вороного

Для каждого примитива триангуляции (треугольника) задаётся весовой центр. Все весовые центры треугольников, имеющие общую точку, объединяются в многоугольник по порядку увеличения радиуса относительно общей точки триангуляции.



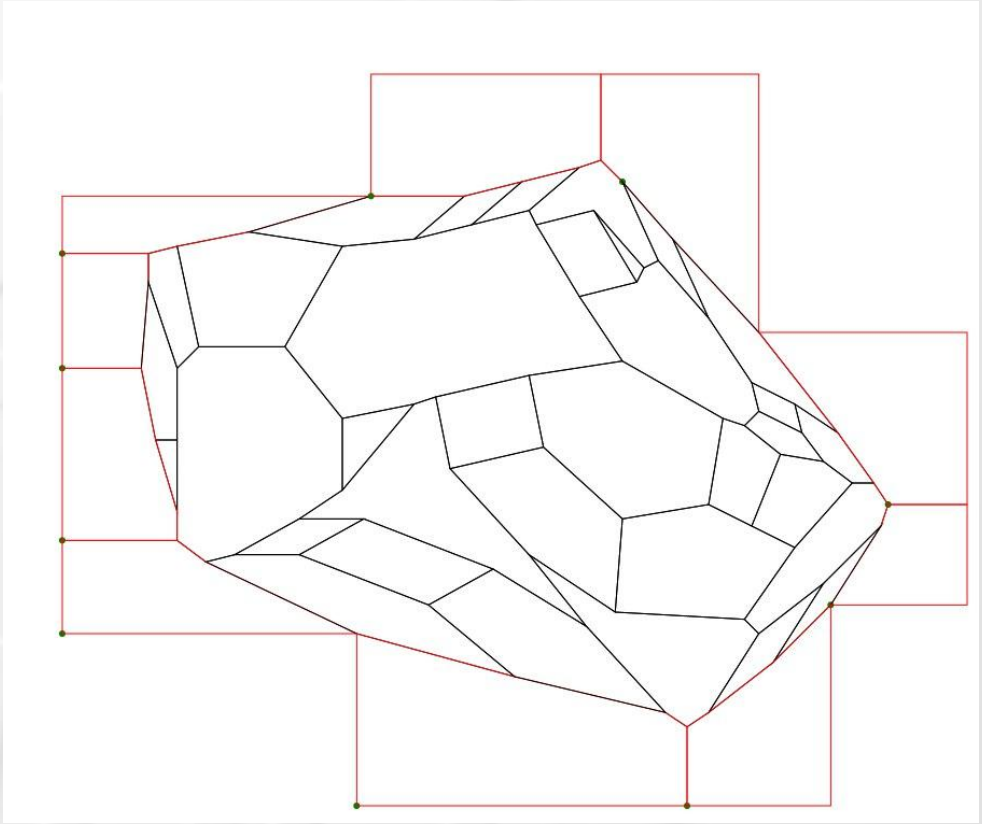
Построение диаграммы Вороного

Для каждого примитива триангуляции (треугольника) задаётся весовой центр. Все весовые центры треугольников, имеющие общую точку, объединяются в многоугольник по порядку увеличения радиуса относительно общей точки триангуляции.



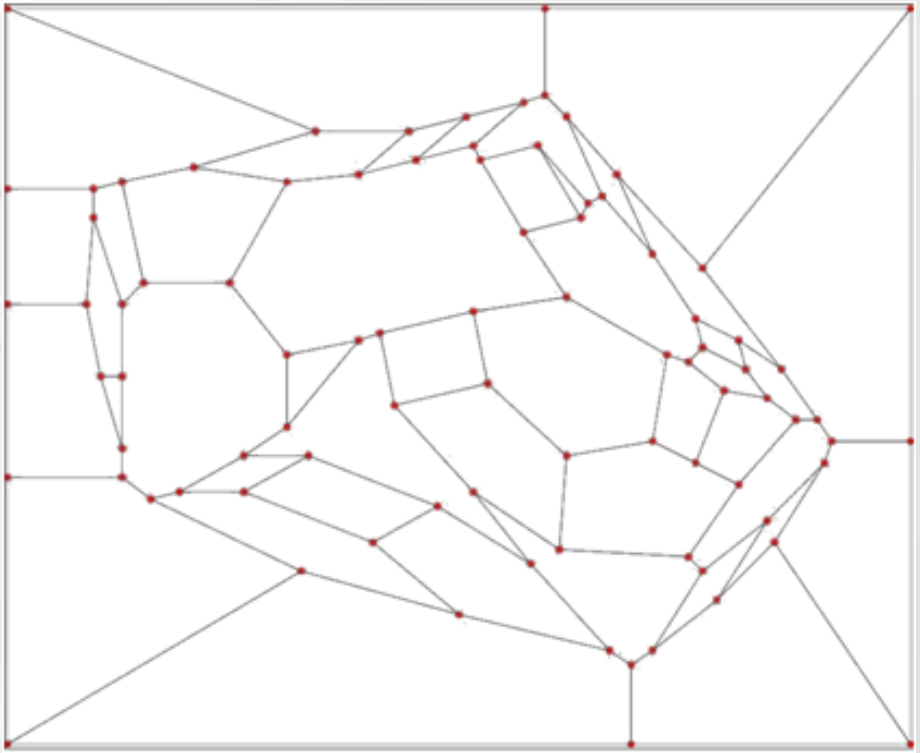
Построение диаграммы Вороного

Для каждого хоста, который принадлежит выпуклой оболочке, строится внешний многоугольник, вписанный в прямоугольник.



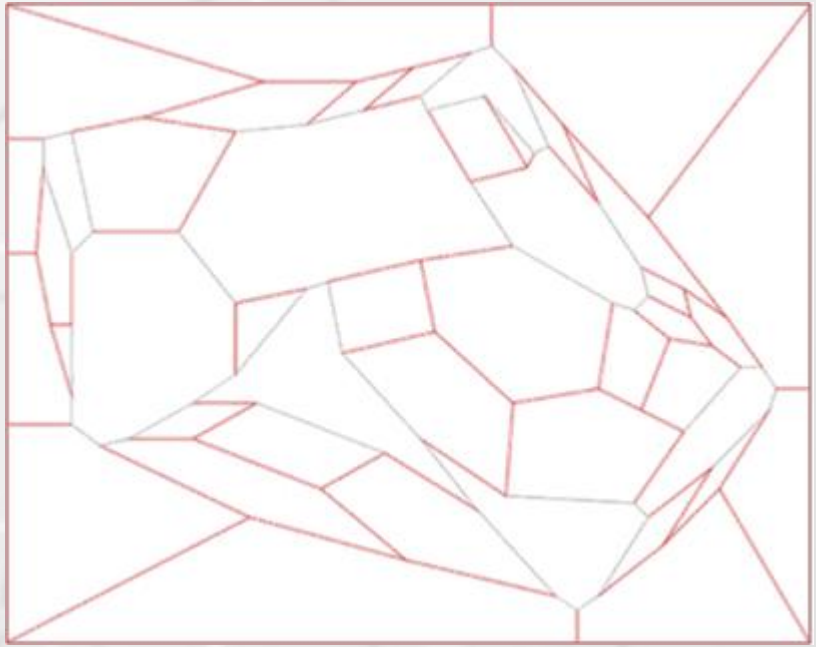
Построение диаграммы Вороного

Для каждого хоста, который принадлежит выпуклой оболочке, строится внешний многоугольник, вписанный в прямоугольник.



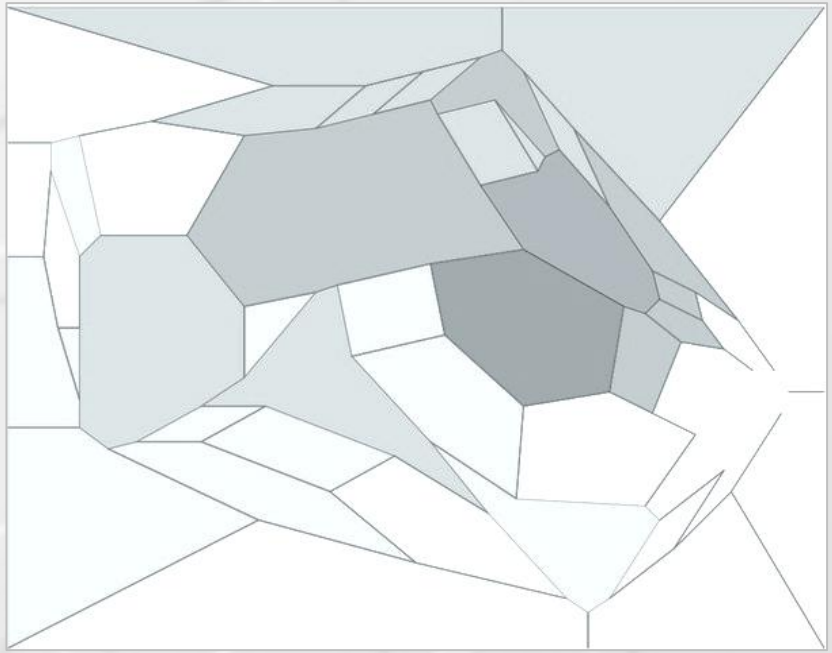
Построение диаграммы Вороного

Каждая общая сторона многоугольников проверяется на соответствие отношений в графе. Если хосты в графе не имеют отношений, на месте отношения прямоугольников строится многоугольник сепаратор (на изображение сепараторы имеют 2 точки).



Построение диаграммы Вороного

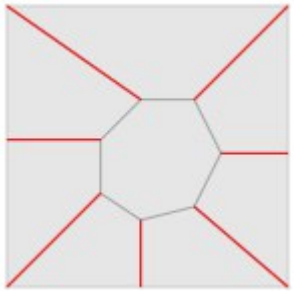
Ячейки диаграммы Вороного закрашиваются в соответствии со значениями метрик хостов. На данном примере, визуализируется дальность хостов от некоторой начальной точки.



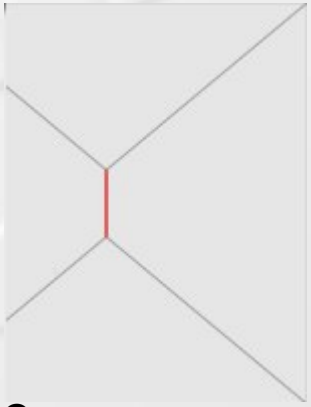
План доклада

- Введение
- Виды визуальных моделей
- Построение диаграммы Вороного
- **Выводы**

Примеры топологий



Звезда



Кольцо

Спираль

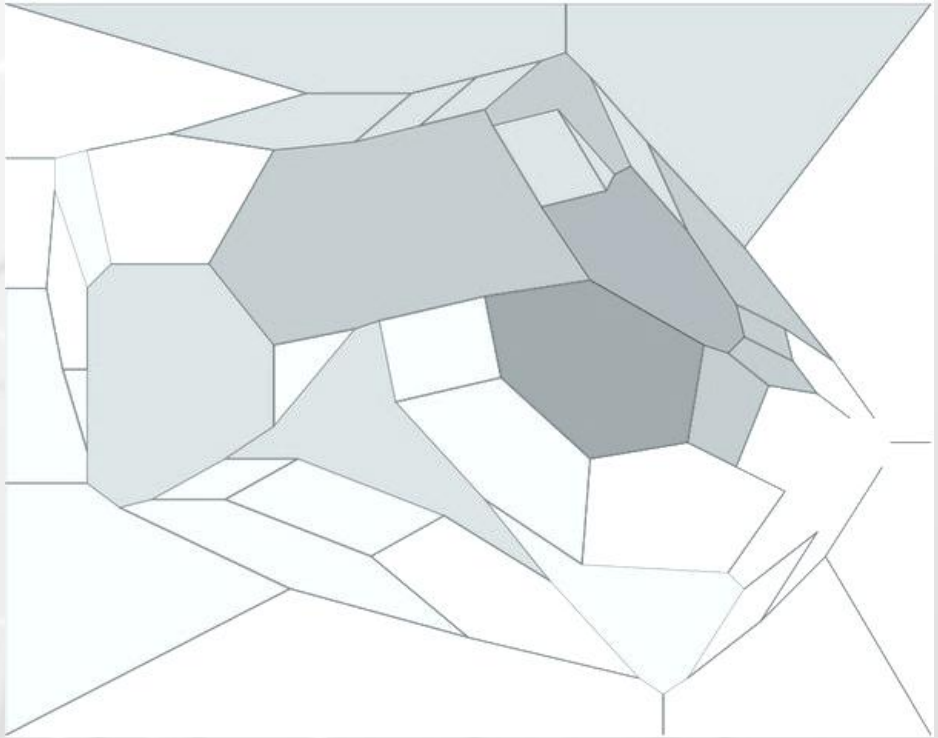
Полносвязный граф

Недостатки

-Граф должен быть планарным. (частично решается приведением к планарности и широкой возможностью вложенности)
- Непривычное отображение затрудняет распознавание отношений. (частично решается обучением)
- Все точки графа должны иметь уникальную координату. (полностью решается фильтром, которые будет преобразовывать входной граф)

Достоинства

+ Широкие возможности вложенности. (отдельная диаграмма вписанная в один из многоугольников)
+Больше возможностей для отображения метрик: размер, цвет, прозрачность, возможность частичного использования 3D, отображение вложенности, разделительные линии.
+Максимум используемого пространства, т.е. минимум информационного шума.
+Эффективное определение кластеров.

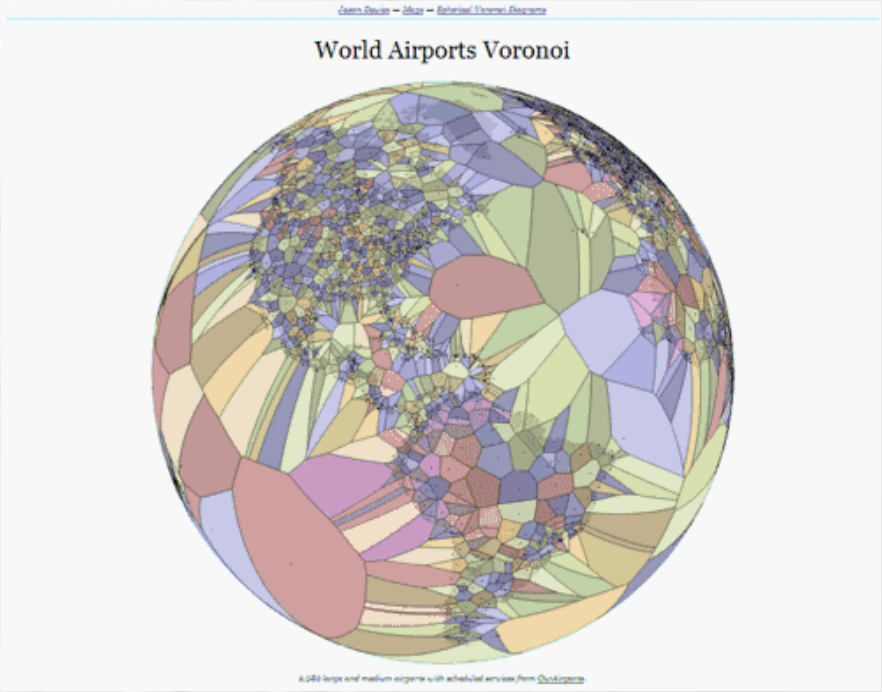


Планы развития

Генератор планарных графов (для тестов)

Фильтр проверяющий граф на планарность и преобразующий его к планарному

Алгоритм и реализация трансформации элементов диаграммы с учётом метрик.



Контактная информация

Чечулин Андрей Алексеевич
andreych@bk.ru
http://comsec.spb.ru/chechulin

Благодарности

Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029.