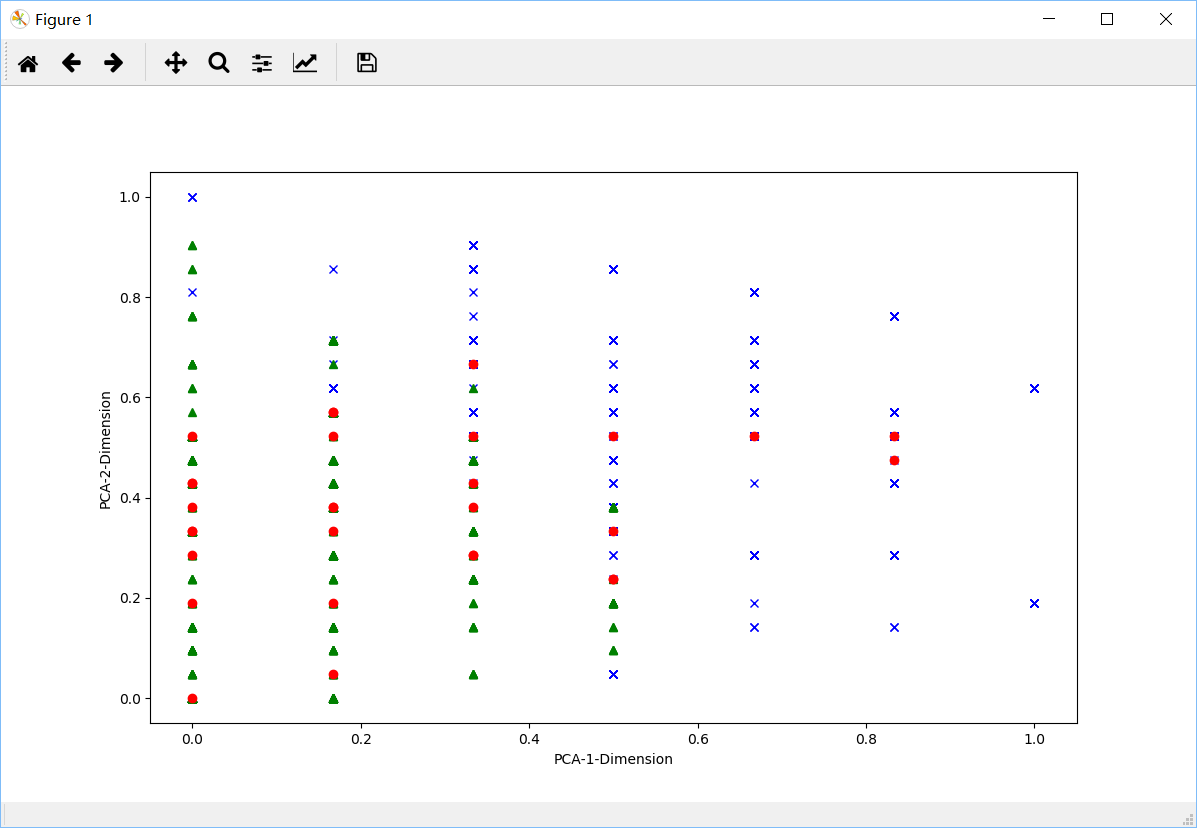
2018年9月28日星期五

下午5时24分

已经下班，自动加班。

随着数据处理开始，自己也着手继续下一步分析。昨天基于CERT5.2中用户离职/解雇的关系数据进行了初步的KMeans聚类分析，但是结果表明无论是PCA还是MinMax都无法挽救该阶段的KMeans，结果如图：



上图为PCA=2时两个维度的图

也许自己不死心吧，决定再次尝试一次，因为论文说“relationship to laid off employees”影响着Job Satisfaction，那么如果直接依据离职人数进行排队呢，不知道场景二的30个用户能排在哪个位置？

首先分析X\_0，即仅考虑同一团队的离职人数，则有：

开始输出Insiders\_2在排序后的索引...

如果考虑X\_1即同一部门内离职人数，依旧不明显

如果考虑LaidOff，依旧结果不明显，此方法作罢。

首先输出X\_0...

30

BYO1846 775

CHP1711 1042

CIF1430 1404

CKP0630 1648

DCC1119 349

GWG0497 1458

HIS1394 463

HMS1658 769

HSN0675 1452

HXP0976 1986

ICB1354 1034

ITA0159 570

JAL0811 1138

KSS1005 1825

LVF1626 105

MCP0611 1555

MDS0680 1654

MGB1235 1964

NAH1366 1557

OKM1092 324

OSS1463 1063

RRS0056 1702

SIS0042 1383

SNK1280 1459

TMT0851 480

TNB1616 447

TRC1838 1155

VCF1602 557

WDT1634 1577

ZIE0741 1830

......<<<<<<分割线>>>>>>......

2018年9月29日星期六

上午10时42分

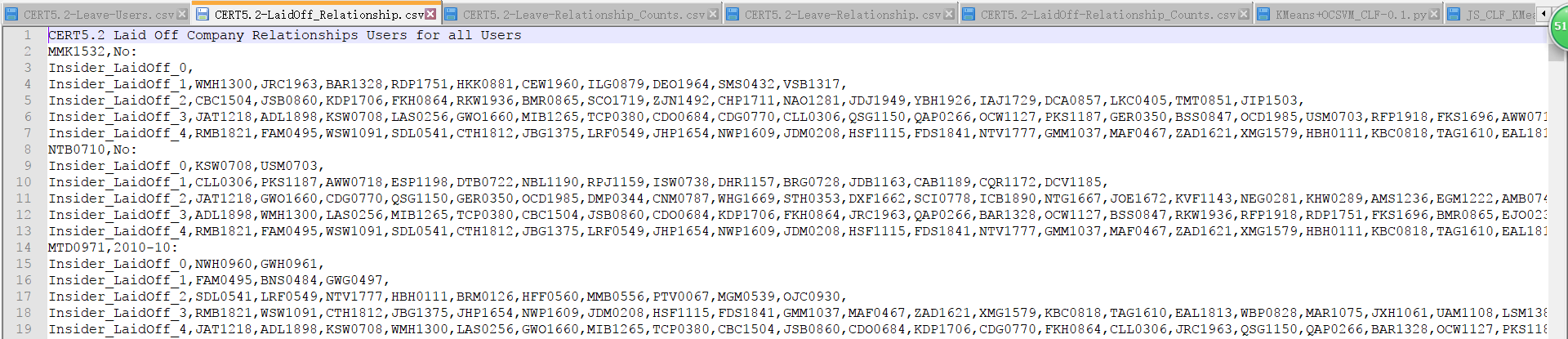
国庆假期调休。

昨天下班时进一步考证了单独从离职人员数量角度无法有效区分，那么看来需要考虑离职人员的亲密度了。

再继续进行下一步前，简单回顾下自己分析离职人员关系的步骤。

1. 统计了LDAP中所有的部门架构层级关系，进而统计了每个部门架构（细化到团队）中的用户成员，得到了CERT5.2-LDAPUsers.csv
2. 在上述基础上，从2009-12的LDAP文件开始，逐个分析到2011--05的LDAP，统计列出这段时间所有离职（工作时间未干全）的员工列表，以及其离职时间（未离职就是NO），得到了CERT5.2-Leave-Users.csv
3. 在上述基础上，重点统计2000个CERT5.2用户的各个层级架构中，出现的离职时间不晚于其离职的用户成员，并分别列入各个层次的列表中，得到CERT5.2-Leave-Relationship.csv；当过滤掉场景二的攻击者后，得到的是CERT5.2-LaidOff-Relationship.csv

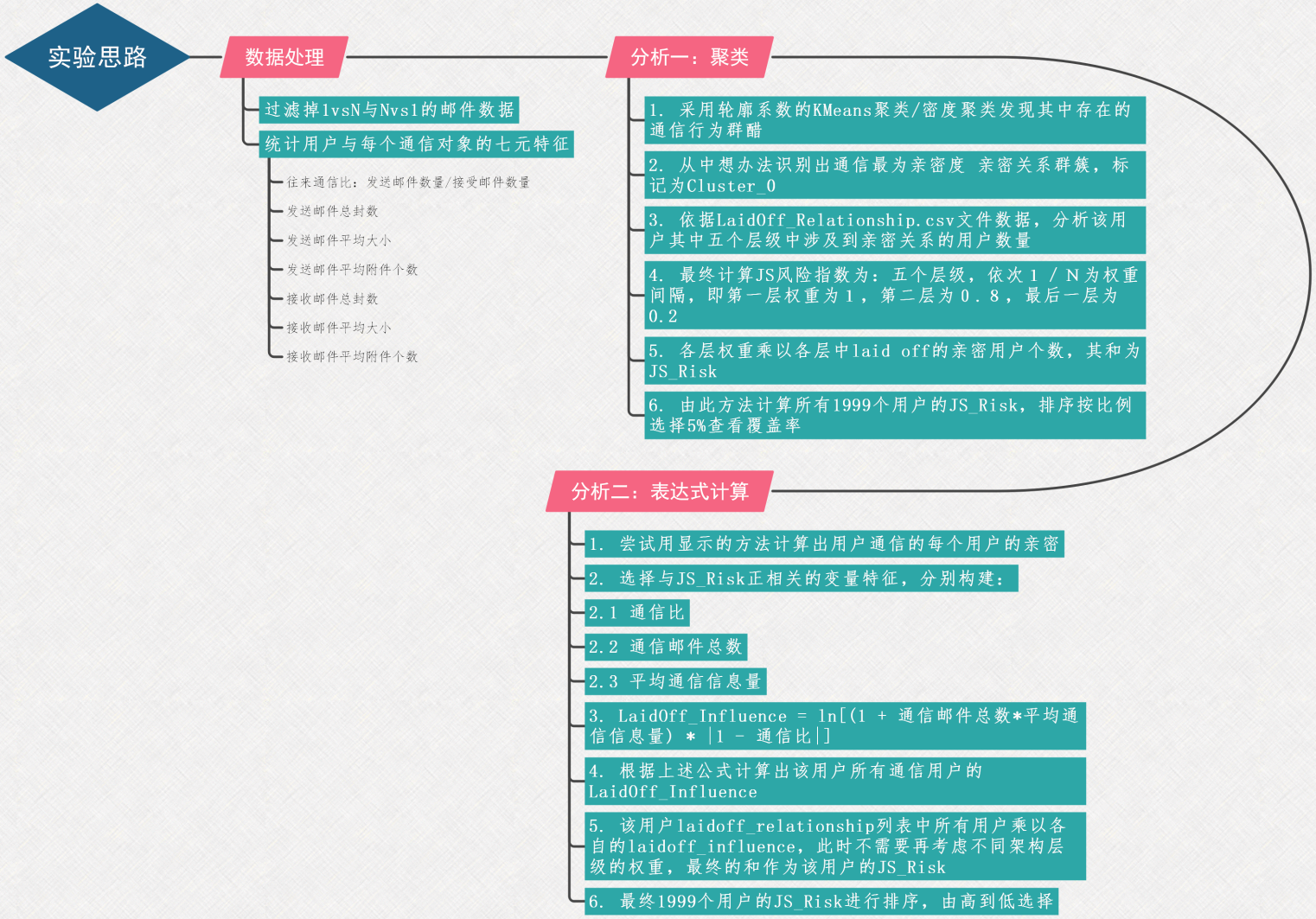
一个简单的示例如：



2018年9月29日星期六

下午2时51分

下午初步整理了下接下来分析的思路，在正式实验前，首先将整体思路放在首位。



完成了单一用户的发送与接收邮件列表，可以看出发送与接收的邮件用户十分不对等

首先统计用户的有效邮件通信列表...

BYO1846 119 发送的邮件用户列表分析完毕...

Macy\_Patterson

Hannah.Mollie.Callahan

Eugenia.Shafira.Mercado

Gareth.Ross.Becker

Xanthus.Kamal.Berger

Micah-King

Tatyana\_A\_Johnston

Jonathan\_Buck

WAS1

Tana\_P\_Orr

BYO1846 42 接收邮件用户列表分析完毕...

Buffy.Yolanda.Ortiz

Kitra.Alexa.Mack

Buffy\_Ortiz

Rose.Maisie.Blackwell

Jonathan.Kasimir.Buck

Olympia.N.Bonner

Kirby.Violet.Pena

Wang.Clark.Rice

Belle.Georgia.Frost

Jemima.Brynne.Pratt

晚上重新修改了程序，结果得到

BYO1846 发送邮件与接收邮件分析完毕...

发送邮件统计示例...

**119 119 （两次结果一样）**

['Macy\_Patterson', 2.0, 5687130.0, 7.0]

['Hannah.Mollie.Callahan', 6.0, 6778336.0, 7.0]

['Eugenia.Shafira.Mercado', 8.0, 11621806.0, 10.0]

['Gareth.Ross.Becker', 5.0, 15104163.0, 12.0]

['Xanthus.Kamal.Berger', 7.0, 14001504.0, 13.0]

['Micah-King', 4.0, 6512878.0, 10.0]

['Tatyana\_A\_Johnston', 1.0, 5938693.0, 6.0]

['Jonathan\_Buck', 2.0, 1627944.0, 2.0]

['WAS1', 6.0, 10403150.0, 10.0]

['Tana\_P\_Orr', 1.0, 2930252.0, 4.0]

接收邮件统计示例...

74 74

['Nelle.Regan.Roman', 14.0, 16731087.0, 20.0] 经过实际验证，NRR确实存在receive邮件

['Nelle.Zephr.Hammond', 6.0, 5106777.0, 7.0]

['Herrod.Bevis.Pearson', 1.0, 1576042.0, 1.0]

['Driscoll.Lewis.Hurst', 1.0, 9091311.0, 8.0]

['YDM6', 4.0, 10587019.0, 12.0]

['Hannah\_M\_Callahan', 11.0, 22461830.0, 24.0]

['WCR66', 1.0, 2053416.0, 2.0]

['Roman-Nelle', 6.0, 9075406.0, 9.0]

['Robert.Merritt.Velez', 26.0, 35519771.0, 41.0]

['Rebekah\_Santos', 15.0, 15771213.0, 17.0]