**README**

The python code extracts data from network communications and identifies edges that have ‘bot-like’ behavior due to repeated communication at equal time intervals.

The code is : *bot\_detection.py*

Read the document “*Botnet Detection Algorithm.docx.pdf*” in the folder for insights on how the algorithm works.

Change the paths of input data in the following functions:

@ get\_Data(day)

• The day input can take [‘a’,’b’,’c’]

• Change this path to point to your input data - *'/Users/emugambi/botnet\_traffic/Data/lanl\_nflow\_a%s'*

• See this folder for all input data files with daily connections between source and destination computers in the LANL network - *'/Users/emugambi/botnet\_traffic/Data/’*

To run the code:

Call this function:

@run\_detection\_methods(which\_day)

*• Which\_day* : select from this list - [‘a’,’b’,’c’]

• Change the path to where you want the results saved

• Results are the edges that show high repetivity and have bot-like behavior

@ edge\_traffic\_dist(which\_day,src,dst)

• Inputs are : [day,source\_computer,destination\_computer]

• Output is a plot of distribution of time intervals between connections.